

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    9 月    5 日  
Date of Application:

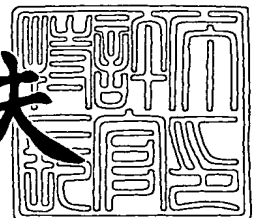
出 願 番 号                      特 願 2 0 0 3 - 3 1 4 4 6 8  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 3 1 4 4 6 8 ]

出      願      人                      株 式 会 社 リ コ ー  
Applicant(s):

2 0 0 3 年 1 0 月    7 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 0 8 2 7 3 0

【書類名】 特許願  
【整理番号】 0304620  
【提出日】 平成15年 9月 5日  
【あて先】 特許庁長官 今井 康夫 殿  
【国際特許分類】 G06F 12/00  
【発明者】  
    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内  
    【氏名】 金井 洋一  
【発明者】  
    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内  
    【氏名】 斉藤 敦久  
【発明者】  
    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内  
    【氏名】 谷内田 益義  
【特許出願人】  
    【識別番号】 000006747  
    【氏名又は名称】 株式会社リコー  
【代理人】  
    【識別番号】 100070150  
    【弁理士】  
    【氏名又は名称】 伊東 忠彦  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2002-269102  
    【出願日】 平成14年 9月13日  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2002-299712  
    【出願日】 平成14年10月11日  
【手数料の表示】  
    【予納台帳番号】 002989  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9911477

**【書類名】 特許請求の範囲****【請求項 1】**

ドキュメントファイルの印刷を行うユーザの属性を取得する手段と、  
上記ドキュメントファイルの属性を取得する手段と、  
取得した上記ユーザおよび上記ドキュメントファイルの属性に基づき、印刷許否および印刷要件を規定したセキュリティポリシーを検索して印刷要件を取得する手段と、  
取得した上記印刷要件を印刷時に強制する手段とを備えたことを特徴とするドキュメント印刷装置。

**【請求項 2】**

上記セキュリティポリシーを上記ドキュメント印刷装置内部に有する請求項 1 に記載のドキュメント印刷装置。

**【請求項 3】**

サーバ上に配置した上記セキュリティポリシーを参照する請求項 1 に記載のドキュメント印刷装置。

**【請求項 4】**

上記セキュリティポリシーを参照し、上記ドキュメントファイルの印刷処理を実行するドキュメント印刷プログラムを備えた請求項 3 に記載のドキュメント印刷装置。

**【請求項 5】**

ドキュメント印刷プログラムは、  
暗号化された上記ドキュメントファイルの復号鍵を取得する手段と、  
取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、  
上記印刷要件をネットワークを介してサーバから取得する手段と、  
取得した上記印刷要件を満たす印刷処理を実行させる手段とを有する請求項 4 に記載のドキュメント印刷装置。

**【請求項 6】**

上記ドキュメントファイルの属性を上記ドキュメントファイルと関連付けて登録するセキュリティ属性データベースをサーバに備えた請求項 5 に記載のドキュメント印刷装置。

**【請求項 7】**

上記ドキュメントファイルの属性は文書カテゴリと機密レベルとを含み、上記ユーザの属性はカテゴリとレベルとを含む請求項 6 に記載のドキュメント印刷装置。

**【請求項 8】**

上記ドキュメントファイルを暗号化した暗号鍵に相当するパラメータをネットワークを介してサーバから取得し、このパラメータから復号鍵を導出する請求項 5 に記載のドキュメント印刷装置。

**【請求項 9】**

内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項 8 に記載のドキュメント印刷装置。

**【請求項 10】**

上記ドキュメントファイルに含まれるパラメータを上記復号鍵の生成に利用する請求項 8 または 9 のいずれか一項に記載のドキュメント印刷装置。

**【書類名】明細書****【発明の名称】ドキュメント印刷装置****【技術分野】****【0001】**

本発明は、文書に関するセキュリティポリシーに基づき印刷を行うドキュメント印刷装置に関する。

**【背景技術】****【0002】**

オフィスに代表されるような文書（ドキュメント）を扱うフィールドでは、その文書のセキュリティをコントロールしたいという要望は常に存在する。現実には多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。文書に関するセキュリティポリシーに基づいて印刷を行う方法に関する従来技術としては、以下のものが挙げられる。

**【0003】**

特許文献1では、データファイルへのアクセスに対応するポリシー、その評価を行う手段に加えて、ポリシーに条件が記述してあって、その条件をクリアにするための実行手段がある場合にはそれを執行することで評価を行うアクセス制御システムの技術が開示されている。

**【0004】**

特許文献2では、ポリシー、システム、制御手段から構成されていて、それぞれの組み合わせを登録してあるデータベースから制御手段を抽出して、システムをポリシーにあうように制御する手段、その状態を監査する手段を有するセキュリティ管理システムの技術が開示されている。

【特許文献1】特開2001-184264号公報

【特許文献2】特開2001-273388号公報

**【発明の開示】****【発明が解決しようとする課題】****【0005】**

オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティの設定を行う方法では、さまざまな機器のセキュリティに関する知識が必要であり、すべての機器にセキュリティを一つ一つ設定する必要がある上、全体がどのようなセキュリティ状態になっているのかが把握しにくく、個々の機器の設定ができていても、実際に文書のセキュリティが守られていることが実感できないなどの問題がある。

**【0006】**

特許文献1に開示されている技術は、データファイルへのアクセス制御システムであって、アクセス後のデータの処理、特に印刷などには言及されていない。

**【0007】**

また、特許文献2に開示されている技術において、そして、システムをポリシーにあうように制御する手段を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低いという問題がある。

**【0008】**

本発明は、上記事情に鑑みてなされたものであり、文書印刷のセキュリティ設定に関して、機器のセキュリティに関する知識が必要である、一つ一つの機器にセキュリティを設定する必要がある、全体のセキュリティ状態が把握できない、実際の文書のセキュリティが守られているかが実感できない、などの問題を解決することを目的とする。

**【課題を解決するための手段】****【0009】**

上記の目的を達成するため、本発明のドキュメント印刷装置は、ドキュメントファイル

の印刷を行うユーザの属性を取得する手段と、上記ドキュメントファイルの属性を取得する手段と、取得した上記ユーザおよび上記ドキュメントファイルの属性に基づき、印刷許可および印刷要件を規定したセキュリティポリシーを検索して印刷要件を取得する手段と、取得した上記印刷要件を印刷時に強制する手段とを備えるようにしている。

【0010】

これにより、印刷時におけるセキュリティ対策を強制することができる。

【0011】

また、上記セキュリティポリシーを上記ドキュメント印刷装置内部に有するものとしてすることができる。これにより、ドキュメント印刷装置と一体にセキュリティポリシーを管理することができる。

【0012】

また、サーバ上に配置した上記セキュリティポリシーを参照するようにすることができる。これにより、多数のドキュメント印刷装置が設置された環境においてもセキュリティポリシーを一元的に管理することができる。

【0013】

また、上記セキュリティポリシーを参照し、上記ドキュメントファイルの印刷処理を実行するドキュメント印刷プログラムを備えるようにすることができる。これにより、印刷時のセキュリティに関する処理を一括に行わせることができる。

【発明の効果】

【0014】

本発明によれば、文書印刷のセキュリティ設定に関して、機器のセキュリティに関する知識は不要となり、一つ一つの機器にセキュリティを設定する必要をなくすることができる。

【0015】

また、全体のセキュリティ状態を把握することができ、実際の文書のセキュリティが守られているかを実感することができる。

【発明を実施するための最良の形態】

【0016】

以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。

【0017】

なお、以下の説明では「プリンタ」という用語を用いているが、これは狭義のプリンタ専用機に限らず、コピー、ファクシミリ、これらの複合・融合された機器等、すなわち印刷機能を有するあらゆる機器を意味するものである。

【0018】

〔第1の実施形態〕

図1は本発明を好適に実施した第1の実施形態にかかるプリンタの内部構成を示す図である。

【0019】

図1において、プリンタ1は、電子的に記述されたセキュリティポリシー2と、印刷処理を実行する印刷部3と、ドキュメントの印刷を要求したユーザの属性（カテゴリ、セキュリティレベル）を取得するユーザ属性取得部4と、印刷対象ドキュメントの属性（カテゴリ、セキュリティレベル）を取得する文書属性取得部5とを含んでいる。印刷指示部6はユーザの要求に基づいて印刷指示を行うとともに、ユーザおよびドキュメントの属性をプリンタ1に通知する部分である。

【0020】

セキュリティポリシー2は、例えば図2に示すような文書で表現されたものを電子的に記述したものである。

【0021】

図3はXML (eXtensible Markup Language) により記述したセキュリティポリシー2の例を示したものである。

**【0022】**

図3に示したセキュリティポリシー2は、前半において、ドキュメントのカテゴリに関わりなく(<doc\_category>ANY</doc\_category>)、ドキュメントのセキュリティレベルがbasicの時は(<doc\_security\_level>basic</doc\_security\_level>)、ユーザのカテゴリにかかわらず(<user\_category>ANY</user\_category>)、ユーザのセキュリティレベルに関わりなく(<user\_security\_level>basic</user\_security\_level>)、印刷は要件なく許可する(<name>print</name><allowed/>)、という条件を表している。

**【0023】**

また、後半において、ドキュメントのカテゴリにかかわらず(<doc\_category>ANY</doc\_category>)、ドキュメントのセキュリティレベルがhighのときは(<doc\_security\_level>high</doc\_security\_level>)、ユーザのカテゴリがドキュメントのカテゴリと同じで(<user\_category>DOC-CATEGORY</user\_category>)、ユーザのセキュリティレベルに関わりなく(<user\_security\_level>basic</user\_security\_level>)、印刷は、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可する(<name>print</name><requirement>audit</requirement><requirement>embed\_trace\_info</requirement>)、という条件を表している。

**【0024】**

以下、図1に基づいて第1の実施形態の動作を説明する。

**【0025】**

印刷にあたり、ユーザの要求に基づいて印刷指示部6からプリンタ1にドキュメントの印刷指示が出されると、ユーザ属性取得部4は印刷指示部6からユーザのカテゴリ、セキュリティレベルを取得し、印刷部3に通知する。文書属性取得部5は印刷指示部6からドキュメントのカテゴリ、セキュリティレベルを取得し、印刷部3に通知する。そして、印刷部3はユーザ属性取得部4と文書属性取得部5とから与えられたユーザおよびドキュメントのカテゴリとセキュリティレベルとからセキュリティポリシー2の対応するエントリを検索し、印刷時に強制する要件(印刷要件)を抽出する。

**【0026】**

図3に示したセキュリティポリシー2に基づくならば、例えばセキュリティレベルが「basic」のドキュメントを印刷しようとしていれば、要件はない。例えばセキュリティレベルが「high」のドキュメントを印刷しようとしていれば、要件として「ログを記録すること」と「追跡可能な情報を埋め込むこと」が要件となる。

**【0027】**

要件がない場合、印刷部3はドキュメントの印刷を行って終了する。例えば上記の例でセキュリティレベルが「basic」の場合に該当する。要件がある場合、印刷部3はその要件をすべて満たすことができるかを判定する。すべての要件を満たすことができない場合は、ユーザに通知をして、印刷をせずに終了する。すべての要件を満たすことができる場合は、その要件を満たして印刷を行い終了する。例えば上記の例でセキュリティレベルが「high」の場合に該当する。すなわち、ログを記録し、追跡可能な情報の埋め込み(電子透かし、バーコードの追加など)を行って、印刷を行い終了する。

**【0028】**

印刷要件には、電子透かしやバーコードの追加、通常とは異なる紙への印刷、ログを記録する等がある。例えば、電子透かしは、一般には音楽や画像などのデジタルデータに著作物に関する情報等を埋め込む場合に用いられる技術である。バーコードと同様、電子透かしを用いて、ドキュメントへ情報を埋め込むことができる。通常とは異なる紙とは、通常時に印刷する白紙の用紙ではない、特別な紙のことである。つまり、通常の白紙と区別をつけることができる紙であって、例えば色紙などがある。

**【0029】**

以上の動作によって、予め定めたセキュリティポリシー2に基づく印刷要件をドキュメントの印刷時において自動的に強制することができる。この場合、文書印刷のセキュリティ設定に関して、機器のセキュリティに関する知識は不必要である。一つ一つの機器にセ

セキュリティを設定する必要もない。さらに、全体のセキュリティ状態を把握させることができ、実際の文書のセキュリティが守られていることをユーザに実感させることができる。

#### 【0030】

##### 〔第2の実施形態〕

図4は本発明を好適に実施した第2の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

#### 【0031】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末401、ユーザ端末402、プリンタ403およびアクセスコントロールサーバ404を有する。

#### 【0032】

配布者端末401およびユーザ端末402は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、配布者端末401にはドキュメント保護プログラム411が、プリンタ403にはドキュメント印刷プログラム421がそれぞれ実装されている。

#### 【0033】

ドキュメント保護プログラム411は、ドキュメントファイルに配布者端末401の使用者（配布者）の入力操作に応じた処理要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEAなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。図5はドキュメント保護プログラム411の構成例を示したものであり、暗号化部411aと暗号鍵取得部411bと属性付与部411cと属性登録部411dとを含んでいる。各部の機能については後の動作において説明する。

#### 【0034】

ドキュメント印刷プログラム421は、ユーザ端末402の使用者（ユーザ）からの印刷要求時に、保護ドキュメントを復号するとともに設定されている印刷要件に応じた印刷処理をプリンタ403に実行させる処理を行うプログラムである。図6はドキュメント印刷プログラム421を有したプリンタ403の構成例を示したものであり、ドキュメント印刷プログラム421は復号部421aと復号鍵取得部421bと印刷要件取得部421cと印刷処理部421dとを含んでおり、プリントエンジン403aに印刷データを渡すようになっている。また、図7は図6における印刷処理部421dの構成例を示したものであり、要件処理部421eとドキュメント加工部421fとプリンタドライバ421gと警告表示部421hとログ記録部421iとを含んでいる。各部の機能については後の動作において説明する。

#### 【0035】

図4に戻り、アクセスコントロールサーバ404は、ユーザがドキュメントを印刷しようとする場合に、プリンタ403内のドキュメント印刷プログラム421からの要求に応じて自身が記録保持しているセキュリティポリシー444を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。図8はアクセスコントロールサーバ404の構成例を示したものであり、属性DB登録部404aとユーザ認証部404bとアクセス権限確認部404cと印刷要件取得送付部404dとを含んでいる。各部の機能については後の動作において説明する。

#### 【0036】

なお、配布者の入力操作に応じてドキュメント保護プログラム411がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、BDPという）、機密印刷（Private Access：以下、PACという）、電子透かし（Digital Watermark：以下、DWMという）の付加、バーコード付加（Embedding Barcode：以下、EBCという）、機密ラベルスタンプ（Security Label Stamp：以下、SLSという）などが挙げられる。

**【 0 0 3 7 】**

図 9 に、アクセスコントロールサーバ 4 0 4 に登録されるセキュリティポリシー 4 4 4 の例を示す。組織におけるセキュリティポリシーは、ドキュメントに対して機密レベル (Sensitivity) および分野 (Category) を設定した上で、ドキュメントに対するアクセスを許可するユーザの階級 (Level) や部門 (Category) およびその印刷要件を設定したものである。図 9 では、例えば、カテゴリが「技術 (Technical)」で機密レベルが「マル秘 (Secret)」のドキュメントファイルは、カテゴリが「技術 (Technical)」で階級が「中 (Medium)」又は「上 (High)」のユーザに対して、閲覧は許可するが RAD を要件とすること、印刷を許可するが PAC と BDP と EBC と RAD とを要件とすること、および、ハードコピーは許可しないことが規定されている。

**【 0 0 3 8 】**

アクセスコントロールサーバ 4 0 4 は、セキュリティポリシー 4 4 4 のデータをどのような形で記録保持していても構わない。なお、XML を用いれば、図 1 0 に示すように、簡単に記述できる。

**【 0 0 3 9 】**

図 4 に戻り、アクセスコントロールサーバ 4 0 4 には、ユーザ各人の認証用の情報 (ユーザ名とパスワードとの組) が格納されたユーザデータベース 4 4 1 と、各保護ドキュメントにどのようなセキュリティ属性が設定されているかを示す情報およびその保護ドキュメントを復号するための暗号鍵が関連付けられて登録されるセキュリティ属性データベース 4 4 3 とが接続されている。

**【 0 0 4 0 】**

図 1 1 に、ユーザデータベース 4 4 1 に登録される情報の例を示す。

**【 0 0 4 1 】**

図 1 1 においてはユーザごとにカテゴリと階級とを別々の属性として管理する構造としているが、たとえば、Windows (R) Domain のユーザ管理機構を利用してユーザを管理するような場合には、グループアカウントとして Technical\_Medium のようなものを生成し、Ichiro というユーザをそのグループに所属させるようにしてもよい。所属グループの命名規則をこのように設定しておくことで、カテゴリと階級とを管理することが可能となる。

**【 0 0 4 2 】**

次に、本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初に、システム全体の動作について説明する。

**【 0 0 4 3 】**

配布者は、配布者端末 4 0 1 を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

**【 0 0 4 4 】**

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末 4 0 1 の入力装置を操作してドキュメントファイルをドキュメント保護プログラム 4 1 1 に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム 4 1 1 は、セキュリティ属性の設定を配布者に要求する。例えば、ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の表示装置にメッセージを表示するなどして、セキュリティ属性の設定を要求する。図 1 2 はセキュリティ属性の設定を要求する画面の例を示したものであり、文書カテゴリ (技術関連、人事関連等) および機密レベル (極秘、秘、社外秘、公開等) の設定がプルダウンメニュー等から選択することにより行えるようになっている。なお、図 1 2 の画面では保護するドキュメントファイルを指定することもできるようになっている。なお、ここでのセキュリティ属性とは、保護しようとするドキュメントがセキュリティ属性データベース 4 4 3 に登録されているセキュリティ属性のうちのいずれに該当するかを示す情報である。

**【 0 0 4 5 】**

配布者が配布者端末 4 0 1 の入力装置を介してドキュメントファイルにセキュリティ属

性を設定すると、ドキュメント保護プログラム 4 1 1 はこれを取得する。

【 0 0 4 6 】

セキュリティ属性を取得したドキュメント保護プログラム 4 1 1 は、ドキュメントファイルごとに固有のドキュメント ID を生成し、復号に使用する暗号鍵とセキュリティ属性とをこれに関連付けてアクセスコントロールサーバ 4 0 4 へ送信し、登録する。

【 0 0 4 7 】

また、ドキュメント保護プログラム 4 1 1 は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメント ID を付加して保護ドキュメントを生成する。

【 0 0 4 8 】

配布者は、ドキュメント保護プログラム 4 1 1 が生成した保護ドキュメントをユーザに受け渡す。

【 0 0 4 9 】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末 4 0 2 に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末 4 0 2 に読み取らせても良いし、ユーザ端末 4 0 2 が配布者端末 4 0 1 と通信可能である場合には、通信網を介して配布者端末 4 0 1 から保護ドキュメントを取得するようにしてもよい。

【 0 0 5 0 】

ユーザが、ユーザ端末 4 0 2 の入力装置を介してプリンタ 4 0 3 に対して印刷を指示すると、プリンタ 4 0 3 内のドキュメント印刷プログラム 4 2 1 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザ端末 4 0 2 を介してユーザに要求する。例えば、ドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。図 1 3 はユーザ名（ユーザ ID）とパスワードを要求する画面の例を示したものであり、キーボード等によって入力が行えるようになっている。

【 0 0 5 1 】

ドキュメント印刷プログラム 4 2 1 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 4 0 4 へ送信して、ユーザ認証を要求する。

【 0 0 5 2 】

アクセスコントロールサーバ 4 0 4 は、ドキュメント印刷プログラム 4 2 1 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【 0 0 5 3 】

ユーザを特定すると、アクセスコントロールサーバ 4 0 4 は、セキュリティ属性データベース 4 4 3 を参照し、保護ドキュメントに設定されているセキュリティ属性の種類を特定する。

【 0 0 5 4 】

アクセスコントロールサーバ 4 0 4 は、ユーザデータベース 4 4 1 から取得したユーザの階級を示す情報および、ドキュメントに設定されているセキュリティ属性とに基づいて、ドキュメントを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際にはどのような印刷要件が設定されているのかを取得する。

【 0 0 5 5 】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ 4 0 4 は、印刷が許可されていることを示す許可情報とともに、保護ドキュメントを復号するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをドキュメント印刷プログラム 4 2 1 に受け渡す。

【 0 0 5 6 】

アクセスコントロールサーバ 4 0 4 から許可情報とともに、暗号鍵と印刷要件とを取得したドキュメント印刷プログラム 4 2 1 は、暗号鍵を用いて保護ドキュメントを復号してドキュメントファイルに復元する。

【 0 0 5 7 】

そしてドキュメント印刷プログラム 4 2 1 は、印刷要件を満たすようにプリンタ 4 0 3 のプリントエンジン 4 0 3 a に印刷処理を実行させる。例えば、ドキュメントファイルに B D P が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【 0 0 5 8 】

これにより、ドキュメントファイルを印刷する際に、予め設定されたセキュリティ属性に応じた印刷要件を強制することが可能となる。

【 0 0 5 9 】

なお、ユーザが印刷要件について意識していない場合があると共に、印刷要件によっては特定のプリンタでないと処理できないものもあるため、印刷の実行前にその旨の情報がユーザに提供されることが望ましい。図 1 4 はユーザ端末 4 0 2 の表示装置上に表示される確認画面の例を示したものであり、印刷要件と利用できるプリンタとが表示され、使用するプリンタを選択することができるようになっている。

【 0 0 6 0 】

ここで、ドキュメントを保護する際のドキュメント保護プログラム 4 1 1 およびアクセスコントロールサーバ 4 0 4 の動作、および保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム 4 2 1 およびアクセスコントロールサーバ 4 0 4 の動作についてさらに詳しく説明する。

【 0 0 6 1 】

図 1 5 に、ドキュメント保護プログラム 4 1 1 が保護ドキュメントを生成する際の処理を示す。また、図 1 6 に、ドキュメント保護プログラム 4 1 1 およびアクセスコントロールサーバ 4 0 4 の動作の流れを示す。

【 0 0 6 2 】

ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の入力装置における配布者の入力操作によってドキュメントファイルとそのセキュリティ属性とを取得すると、ドキュメントファイルを暗号化および復号するための暗号鍵を生成する。そして、ドキュメント保護プログラム 4 1 1 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【 0 0 6 3 】

さらに、ドキュメント保護プログラム 4 1 1 は、ドキュメントファイルごとに固有のドキュメント I D を暗号化ドキュメントに添付して保護ドキュメントを生成する。

【 0 0 6 4 】

保護ドキュメントを生成した後、ドキュメント保護プログラム 4 1 1 は、配布者端末 4 0 1 の通信機能を用いて、暗号鍵とセキュリティ属性とドキュメント I D とをアクセスコントロールサーバ 4 0 4 へ送信し、これらの登録をアクセスコントロールサーバ 4 0 4 に要求する。

【 0 0 6 5 】

暗号鍵とセキュリティ属性とドキュメント I D とをドキュメント保護プログラム 4 1 1 から受け渡されたアクセスコントロールサーバ 4 0 4 は、これらを一つのレコードとしてセキュリティ属性データベース 4 4 3 に記録保持する。

【 0 0 6 6 】

上記の動作を図 5 および図 8 に基づいてさらに詳しく説明する。

【 0 0 6 7 】

まず、図 5 において、ドキュメント保護プログラム 4 1 1 の暗号化部 4 1 1 a は、配布者から引き渡されたドキュメントファイルに対し、暗号鍵取得部 4 1 1 b が生成した暗号鍵を用いて暗号化を行い、この暗号化ドキュメントを属性付与部 4 1 1 c に渡す。

【 0 0 6 8 】

属性付与部 4 1 1 c はドキュメント I D を生成し、暗号化部 4 1 1 a から渡された暗号化ドキュメントにドキュメント I D を付与して保護ドキュメントとして出力する。

【 0 0 6 9 】

また、属性登録部 4 1 1 d は配布者からセキュリティ属性を受け取るとともに、暗号鍵取得部 4 1 1 b から暗号鍵を、属性付与部 4 1 1 c からドキュメント ID をそれぞれ受け取り、アクセスコントロールサーバ 4 0 4 に対してこれらのドキュメント ID、暗号鍵、セキュリティ属性を渡して登録を要求する。

#### 【0 0 7 0】

次いで、図 8 において、アクセスコントロールサーバ 4 0 4 の属性 DB 登録部 4 0 4 a は、渡されたドキュメント ID、暗号鍵、セキュリティ属性をセキュリティ属性データベース 4 4 3 に登録する。

#### 【0 0 7 1】

なお、ドキュメント保護プログラム 4 1 1 がドキュメント ID を生成して暗号化ドキュメントに添付する場合を例に挙げたが、SHA-1 などのハッシュアルゴリズムを用いて暗号化ドキュメントファイルを生成した場合には、そのハッシュ値をドキュメント ID の代わりに用いてもよい。この場合は、保護ドキュメントにドキュメント ID を添付する必要はなく、後でドキュメント ID を取得したい時は、再度ハッシュ値を計算すればよい。

#### 【0 0 7 2】

また、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメント保護プログラム 4 1 1 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 4 0 4 や不図示のサーバなどで行っても良い。

#### 【0 0 7 3】

また、配布者端末 4 0 1 とアクセスコントロールサーバ 4 0 4 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

#### 【0 0 7 4】

ドキュメント保護プログラム 4 1 1 がアクセスコントロールサーバ 4 0 4 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (R) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしてもよい。その場合、アクセスコントロールサーバ 4 0 4 は、例えば「register(String docId, byte[] key, byte[] acl)」のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTPS の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保することができる。

#### 【0 0 7 5】

次に、ドキュメント印刷プログラム 4 2 1 が保護ドキュメントを印刷する際の動作について説明する。図 1 7 に、ドキュメント印刷プログラム 4 2 1 およびアクセスコントロールサーバ 4 0 4 の動作の流れを示す。

#### 【0 0 7 6】

プリンタ 4 0 3 内のドキュメント印刷プログラム 4 2 1 は、ユーザ端末 4 0 2 の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメント ID を取得する。

#### 【0 0 7 7】

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ (ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print” となる。) とをアクセスコントロールサーバ 4 0 4 へ送信して、アクセス権限があるか否かのチェックを要求する。なお、図 1 8 はアクセスコントロールサーバ 4 0 4 への SOAP による問い合わせの例を示す図であり、ユーザ名 (userId) とドキュメント ID (docId) とアクセスタイプ (accessType) とを渡してアクセスが許可されているかを問い合わせる SOAP メッセージ (isAllowed) を送付し、その結果 (isAllowedResponse) を受け取っている例である。結果には、許可されているということ (allowed が true) と要件 (requirements) とが含まれている。

**【0078】**

アクセスコントロールサーバ404は、ドキュメント印刷プログラム421からユーザ名とパスワードとドキュメントIDとアクセスタイプとを取得すると、ユーザデータベース441に登録されている情報を参照し、ユーザ認証を行う。

**【0079】**

換言すると、アクセスコントロールサーバ404は、ユーザデータベース441に登録されている情報を参照し、ドキュメント印刷プログラム421から取得した情報に含まれるユーザ名とパスワードとの組と一致するものが、ユーザデータベース441に登録されているか否かを判断する。

**【0080】**

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム421から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース441に登録されていない場合）、アクセスコントロールサーバ404は、許可情報を「不許可」としてプリンタ403内のドキュメント印刷プログラム421へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム421へ受け渡すようにしてもよい。

**【0081】**

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ404は、セキュリティ属性データベース443に登録されているレコードのうち、ドキュメント印刷プログラム421から取得した情報に含まれるドキュメントIDに関するレコードを読み出す。また、アクセスコントロールサーバ404は、ユーザデータベース441からユーザの「階級」および「部門」を取得する。

**【0082】**

アクセスコントロールサーバ404は、読み出したレコードに基づいてドキュメントファイルに設定されているセキュリティ属性（すなわち、機密レベルおよびカテゴリ）を取得する。そして、自身が記録保持しているセキュリティポリシー444とレコードから読み出したセキュリティ属性に基づいて、ユーザがドキュメントに対してアクセスタイプで示される処理を行う場合の可否を示す許可情報とユーザがドキュメントを印刷する際の印刷要件を取得する。

**【0083】**

ユーザにドキュメントファイルを印刷する権限がある場合は、セキュリティポリシー444として設定されている許可情報は「許可」であるため、アクセスコントロールサーバ404は、レコードに格納されていた暗号鍵と印刷要件とを許可情報とともにプリンタ403のドキュメント印刷プログラム421に受け渡す。

**【0084】**

一方、ユーザにドキュメントファイルを印刷する権限がない場合は、セキュリティポリシー444として設定されている許可情報は「不許可」であるため、アクセスコントロールサーバ404は、許可情報のみをプリンタ403のドキュメント印刷プログラム421に受け渡す。

**【0085】**

次いで、ドキュメント印刷プログラム421は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PACが指定されていれば機密印刷モードに設定する）、プリントエンジン403aにドキュメントファイルの印刷処理を実行させる。

**【0086】**

なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

**【0087】**

アクセスコントロールサーバ404から取得した印刷要件を満足する印刷をプリンタ403では実行できない場合、換言すると、プリンタ403がセキュリティポリシー444

として設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

#### 【0088】

上記の動作を図6～図8に基づいてさらに詳しく説明する。

#### 【0089】

まず、図6において、プリンタ403内のドキュメント印刷プログラム421の復号鍵取得部421bはアクセスコントロールサーバ404に対してアクセス権の確認を行う。

#### 【0090】

確認の問い合わせを受けたアクセスコントロールサーバ404は、図8において、ユーザ認証部404bがユーザデータベース441を参照してユーザ認証を行い、認証結果をアクセス権限確認部404cに通知する。また、ユーザ認証に成功した場合、アクセス権限確認部404cがセキュリティ属性データベース443およびセキュリティポリシー444を参照して許可情報および復号鍵を取得するとともに、印刷要件取得送付部404dがセキュリティポリシー444から印刷要件を取得し、ドキュメント印刷プログラム421に通知する。なお、図8では許可情報、復号鍵および印刷要件を別々に返すようにしているが、これらを一度に返すようにしてもよい。

#### 【0091】

図6において、復号鍵取得部421bはアクセス権の確認ができた場合にアクセスコントロールサーバ404から復号鍵を得て、これを復号部421aに渡す。また、印刷要件取得部421cはアクセスコントロールサーバ404から印刷要件を取得し、印刷処理部421dに渡す。

#### 【0092】

復号部421aは復号鍵取得部421bから取得した復号鍵を用いて保護ドキュメントを復号し、ドキュメントファイルを得て印刷処理部421dに渡す。

#### 【0093】

次いで、図7において、印刷処理部421dの要件処理部421eは、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述したBDP、EBC、SLSのようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部421fに加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ421gに渡し、印刷データをプリントエンジン403aに与えて印刷を行う。また、PACのようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ421gに印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部421hに警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部421iにログ情報を渡し、リモートサーバ等にログデータを登録させる。

#### 【0094】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権を判断するシステム構成においては、アクセスコントロールサーバ404に登録されているセキュリティポリシー444を配布者端末401やアクセスコントロールサーバ404における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布したあとで印刷要件を変更したりすることが可能となる。

#### 【0095】

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

#### 【0096】

なお、ドキュメントファイルを印刷する際に、ドキュメント印刷プログラム421が必ずアクセスコントロールサーバ404に対してセキュリティポリシーを問い合わせる方式とすると、ユーザ数の増加に伴いアクセスコントロールサーバ404の情報処理量が増え

、負担が大きくなってしまう。

【0097】

このため、アクセスコントロールサーバ404の機能の一部をドキュメント印刷プログラム421に移行してもよい。

【0098】

例えば、ドキュメント印刷プログラム421は、ユーザ認証を行った上で、ドキュメントIDをアクセスコントロールサーバ404へ受け渡すと、セキュリティポリシーと暗号鍵とセキュリティ属性とをアクセスコントロールサーバ404から取得し、これを基に許可情報や印刷要件を判断して処理するようにしてもよい。

【0099】

このようにすれば、アクセスコントロールサーバ404の情報処理量を減らし、システム動作上の負担を軽減できる。この場合は、セキュリティポリシーに基づいた判断をドキュメント印刷プログラム421が行うため、ドキュメントにセキュリティ属性を添付した後に暗号化して暗号化ドキュメントとし、ドキュメントIDを添付して保護ドキュメントとすることが好ましい。これにより、セキュリティ属性をアクセスコントロールサーバ404で管理する必要がなくなり、システム動作上のアクセスコントロールサーバ404の負担をさらに軽減できる。

【0100】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム421に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号することも可能ではある。この場合は、セキュリティポリシーとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【0101】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム411の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。この場合は、ドキュメント印刷プログラム421にも同一の秘密鍵を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム421のみが、保護ドキュメントを復号して印刷することが可能となる。

【0102】

図19および図20は上述したような内部に秘密鍵を埋め込んでおくタイプの構成例を示したものであり、図19はドキュメント保護プログラム411の構成例を示し、図20はドキュメント印刷プログラム421の構成例のうち復号に関係する部分のみを示している。なお、この例は、単に内部に秘密鍵を埋め込んでおくだけではなく、乱数を導入して不正アクセスに対しより強化している。

【0103】

図19において、ドキュメント保護プログラム411は暗号化部411aと暗号鍵取得部411bと属性付与部411cと属性登録部411dとパラメータ取得部411eとを含んでいる。

【0104】

動作にあつては、パラメータ取得部411eはパラメータ(kp)を生成し、暗号鍵取得部411bに渡す。なお、パラメータ(kp)はドキュメント保護プログラム411の内部に保持しておくか、要求があつた場合に生成するようにする。

【0105】

暗号鍵取得部411bはパラメータ取得部411eからパラメータ(kp)を受け取った上で、二つの乱数(kd)(ks)を生成し、暗号鍵(k)を式 $k=H\{ks, kp, kd\}$ あるいは $k=D\{kd, D\{ks, kp\}\}$ で計算して生成し、暗号鍵(k)を暗号化部411aに、乱数(kd)を属性付与部411cに、乱数(ks)を属性登録部411dにそれぞれ渡す。なお、 $H\{data1, data$

2, ...} は data1, data2, ... のハッシュ値を計算することを意味し、D{data, key} は key で data を復号することを意味している。

#### 【0106】

暗号化部 411a は配布者から引き渡されたドキュメントファイル (doc) に対し、暗号鍵取得部 411b から取得した暗号鍵 (k) を用いて暗号化を行い、暗号化されたドキュメント (enc) を属性付与部 411c に渡す。式で示せば  $enc = E\{doc, k\}$  となる。なお、E{data, key} は key で data を暗号化することを意味している。

#### 【0107】

次いで、属性付与部 411c はドキュメント ID (id) を生成し、暗号化されたドキュメント (enc) にそのドキュメント ID (id) と暗号鍵取得部 411b から渡された乱数 (kd) を付与して保護ドキュメント ( $enc + id + kd$ ) を出力する。また、属性付与部 411c は生成したドキュメント ID (id) を属性登録部 411d に渡す。

#### 【0108】

属性登録部 411d は、属性付与部 411c から渡されたドキュメント ID (id) と暗号鍵取得部 411b から渡された乱数 (ks) と配布者から取得したセキュリティ属性 (attr) とをアクセスコントロールサーバ 404 に通知し、登録を要求することになる。

#### 【0109】

復号にあつては、図 20 において、復号鍵取得部 421b は保護ドキュメントから乱数 (kd) を取得するとともに、パラメータ取得部 421j からドキュメント印刷プログラム 421 の内部に保持してある、あるいは要求に応じて生成したパラメータ (kp) を取得し、さらにアクセスコントロールサーバ 404 から乱数 (ks) を取得し、暗号化の場合と同様に式  $k = H\{ks, kp, kd\}$  あるいは  $k = D\{kd, D\{ks, kp\}\}$  で計算して復号鍵 (暗号鍵) (k) を得る。

#### 【0110】

そして、復号部 421a は暗号化されたドキュメント (enc) を復号鍵 (k) で復号し、ドキュメントファイル (doc) を得る。

#### 【0111】

図 19 および図 20 は、アクセスコントロールサーバ 404 に登録される乱数 (ks) と保護ドキュメント内の乱数 (kd) とドキュメント保護プログラム 411 もしくはドキュメント印刷プログラム 421 内から取得されるパラメータ (kp) とに基づいて暗号鍵 (復号鍵) (k) を生成する方式であるが、こうすることでアクセスコントロールサーバ 404 が悪意のあるユーザによって不正アクセスされて乱数 (ks) が知られてしまった場合であっても、乱数 (kd) やパラメータ (kp) が知られなければ保護ドキュメントを復号できないことになる。なお、アクセスコントロールサーバ 404 が不正アクセスされないように十分にガードされている環境にあつては、乱数 (ks) をそのまま暗号鍵 (復号鍵) (k) として使用してもよい。

#### 【0112】

一方、これまで説明してきた第 2 の実施形態では、印刷要件をアクセスコントロールサーバ 404 にのみ格納するものとしてきたが、そのような形式に限定されず、保護ドキュメントに含めるようにしてもよい。例えば、ユーザによらずドキュメントファイルに対して必ず指定するような印刷要件については保護ドキュメントの中に含めるようにしてもよい。

#### 【0113】

図 21 は、印刷要件を保護ドキュメントに含める第一印刷要件と、アクセスコントロールサーバ 404 に格納される第二印刷要件とに分けた場合のドキュメント印刷プログラム 421 の構成例を示したものであり、印刷要件取得部 421c においてアクセスコントロールサーバ 404 から第二印刷要件を取得するとともに、復号部 421a において保護ドキュメントから第一印刷要件を取得し、第一印刷要件および第二印刷要件に基づいて印刷処理部 421d で印刷処理を行うようにしている。その他は図 6 に示したドキュメント印刷プログラム 421 と同様である。

**【0 1 1 4】**

また、本実施形態においては、ドキュメント印刷プログラム 4 2 1 はドキュメントファイルの印刷に関する処理のみを行っているが、ユーザ端末 4 0 2 に対してドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を提供するものとしても良い。例えば、Adobe Acrobat (R) のPlug-inと連携してポータブルドキュメントファイル (Portable Document Format : P D F File) の表示、編集および印刷の機能を実現することが可能である。

**【0 1 1 5】**

このように、本実施形態にかかるドキュメント保護・印刷システムによれば、予めセキュリティポリシーとして設定されている印刷要件をドキュメントを印刷する際に強制することができる。

**【0 1 1 6】**

図 2 2 に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。これらについて第 2 の実施形態におけるシステム構成を例として具体的に説明する。

**【0 1 1 7】**

まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作を図 2 3 に示す。

**【0 1 1 8】**

(1) ドキュメント印刷プログラム 4 2 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 2 4 に示すように、プリントダイアログを表示させた後に個人識別番号 (Personal Identification Number : P I N) を入力するダイアログをユーザ端末 4 0 2 の表示装置に表示させ、ユーザに P I N の入力を要求する。

**【0 1 1 9】**

(2) ユーザ端末 4 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 4 2 1 は、これをプリンタドライバに設定し、印刷を指示する。

**【0 1 2 0】**

プリンタドライバは、ドキュメントから Postscript などの P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバはさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリントエンジン 4 0 3 a に送る。

**【0 1 2 1】**

プリントエンジン 4 0 3 a は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 4 0 3 内部の記憶装置 (HDD など) に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 4 0 3 のオペレーションパネルを介して入力すると、プリンタ 4 0 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件 (部数、トレイなど) を適用しながら P D L データに従って印刷出力する。

**【0 1 2 2】**

(3) プリンタドライバに P I N が設定できない、すなわち、プリンタ 4 0 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

**【0 1 2 3】**

このようにすることで、印刷実行後、プリンタ 4 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 4 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 4 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメン

トの漏洩を防止することが可能となる。さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 4 0 3 とのやりとりを S S L で保護してもよい。

#### 【 0 1 2 4 】

また、ドキュメント印刷プログラム 4 2 1 を Windows ( R ) Domain のユーザ管理と連動させて、ユーザに対して P I N の入力を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows ( R ) Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 4 0 3 へ送付するようにする。プリンタ 4 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで Windows ( R ) Domain のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows ( R ) Domain に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

#### 【 0 1 2 5 】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

#### 【 0 1 2 6 】

( 1 ) ドキュメント印刷プログラム 4 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ ( 又は、二次元コード ) のデータを生成する。

#### 【 0 1 2 7 】

( 2 ) ドキュメント印刷プログラム 4 2 1 は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリントエンジン 4 0 3 a に印刷を指示する。

#### 【 0 1 2 8 】

( 3 ) プリンタドライバに E B C が設定できない、すなわち、プリンタ 4 0 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

#### 【 0 1 2 9 】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にアクセスコントロールサーバ 4 0 4 でハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

#### 【 0 1 3 0 】

次に、印刷要件として B D P が設定されている場合のドキュメント印刷プログラム 4 2 1 の動作について説明する。

#### 【 0 1 3 1 】

( 1 ) ドキュメント印刷プログラム 4 2 1 は、B D P が設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する ( 例えば、Ichiro, 2002/08/04 23:47:10 ) 。

#### 【 0 1 3 2 】

( 2 ) ドキュメント印刷プログラム 4 2 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

#### 【 0 1 3 3 】

( 3 ) ドキュメント印刷プログラム 4 2 1 は、生成した地紋画像をスタンプとしてプリンタドライバにセットし、プリントエンジン 4 0 3 a にドキュメントの印刷を指示する。

#### 【 0 1 3 4 】

( 4 ) プリンタドライバに B D P が設定できない場合、すなわちプリンタ 4 0 3 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択す

るようにユーザに通知し、印刷を行わずに処理を終了する。

【0135】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋画像として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、EBCをサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【0136】

次に、印刷要件としてSLSが設定されている場合のドキュメント印刷プログラム421の動作について説明する。

【0137】

(1) ドキュメント印刷プログラム421は、SLSが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの (Top Secretならば「極秘」のマークなど) を選択する。

【0138】

(2) 選択した画像のデータを、スタンプとしてプリンタドライバにセットし、プリントエンジン403aに印刷を指示する。

【0139】

(3) プリンタドライバにSLSをセットできない場合、すなわち、プリンタ403がSLSをサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0140】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【0141】

上記の各例は、あくまでも印刷要件の例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する (印刷に使用する用紙トレイを特殊用紙のトレイに限定する) ようにしてもよい。

【0142】

さらに付言すると、印刷要件には、機能を制限・禁止するものと、機能を強制的に使用させるもの、加えて通常の印刷条件指定などを含めることができる。機能を制限・禁止する例としては、機密文書原本と区別をするために特別なユーザのみカラーでの印刷を許可して、他のユーザはグレースケールでの印刷のみを許可するように制限するための印刷要件などである。機能を強制的に使用させる例としては、機密印刷モードを強制的に使用するような印刷要件や、ログを強制的に記録するような印刷要件、印刷紙面に印刷したユーザの名前を強制的に印字するような印刷要件、ウォーターマークを強制的に印刷する印刷要件、地紋を強制的に印刷する印刷要件などである。通常の印刷条件を指定する例としては、用紙設定としてA4を指定する印刷要件、再生紙トレイを使用する印刷要件、両面印刷を指定する印刷要件などである。

【0143】

また、これまで印刷要件の表現形式としてRAD、PACといったキーワードを用いて説明してきたが、そのようなキーワードでなくとも、例えば、プリンタドライバに設定する設定ファイルのデータそのものや、プリントデータに挿入するページ記述言語で表現したデータ、画面に表示する文字列そのもの、処理すべき要件の内容をスクリプト言語で記述したデータのようなものを用いて印刷要件を表現して規定するようにしても良い。すなわち、印刷要件の表現をキーワードのようなものに限定するものではない。

【0144】

このように、プリンタ403がサポートする様々なセキュリティ機能を利用してセキュ

リティポリシーに沿った印刷要件を設定することによって、プリンタ 4 0 3 のセキュリティ機能が無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは他の実施形態のシステム構成においても同様である。

#### 【0 1 4 5】

一方、これまでの説明において、保護対象はドキュメント全体であるように記述してきたが、ドキュメントの中に保護対象となる部分（セグメントと呼ぶ）と、保護対象としない部分が混在していても良い。例えば、図 2 5 に示すように、保護セグメントが複数保護ドキュメント内に存在していても良い。この場合、保護セグメントごとに異なるセグメント ID をつけ、これまでの説明におけるドキュメント ID をセグメント ID と読みかえれば、同じ原理で保護セグメントごとに印刷を含むアクセスの制御が可能になる。実際には、保護セグメントの先頭と末尾には、そこから保護セグメントが開始することを示しそこで保護セグメントが終了することを示すマークのようなものをつける必要がある。そういったマークの入れ方については、MIME のマルチパートセパレータなどの従来技術を用いることができる。

#### 【0 1 4 6】

また、これまではドキュメント保護プログラムが配布者端末に配置されるような実施例に基づいて説明してきたが、ドキュメント保護プログラム本体はリモートサーバ上に配置するようにしても良い。例えば図 4 の配布者端末 4 0 1、ドキュメント保護プログラム 4 1 1 およびアクセスコントロールサーバ 4 0 4 の関係は、図 2 6 に示すように変形することができる。このように配置することにより、ドキュメント保護プログラムがインストールされていない端末からでもリモートサーバにドキュメントと必要なパラメータを送付して保護ドキュメントを取得することができる。

#### 【0 1 4 7】

なお、上述した各実施形態は、本発明の好適な実施の例であり、本発明はこれらに限定されることはない。

#### 【0 1 4 8】

例えば、上記実施形態においては、配布者端末とユーザ端末とが別個の装置である場合を例に説明を行ったが、これらは同一の装置を共用するような構成であっても構わない。

#### 【0 1 4 9】

また、ユーザ認証の方法は、ユーザ名とパスワードとを用いる方法に限定されることなく、スマートカードを用いた P K I ベースの認証方法を適用してもよい。

#### 【0 1 5 0】

このように、本発明は様々な変形が可能である。

#### 【図面の簡単な説明】

#### 【0 1 5 1】

【図 1】 本発明を好適に実施した第 1 の実施形態にかかるプリンタの内部構成を示す図である。

【図 2】 セキュリティポリシーの例を示す図である。

【図 3】 セキュリティポリシーを XML 記述により書き表したプログラムの例を示す図である。

【図 4】 本発明を好適に実施した第 2 の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。

【図 5】 ドキュメント保護プログラムの構成例を示す図である。

【図 6】 ドキュメント印刷プログラムを有したプリンタの構成例を示す図である。

【図 7】 印刷処理部の構成例を示す図である。

【図 8】 アクセスコントロールサーバの構成例を示す図である。

【図 9】 セキュリティポリシーを電子データとした場合のデータ構造を示す図である。

。

【図 1 0】 セキュリティポリシーを電子データとして記述した例を示す図である。

【図 1 1】 ユーザデータベースに記録される情報の構造例を示す図である。

【図 1 2】セキュリティ属性の設定を要求する画面の例を示す図である。

【図 1 3】ユーザ名（ユーザ ID）とパスワードを要求する画面の例を示す図である。

【図 1 4】ユーザ端末の表示装置上に表示される確認画面の例を示す図である。

【図 1 5】第 2 の実施形態にかかるドキュメント保護プログラムの処理を示す図である。

【図 1 6】第 2 の実施形態にかかるドキュメント保護プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図 1 7】第 2 の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。

【図 1 8】アクセスコントロールサーバへの S O A P による問い合わせの例を示す図である。

【図 1 9】ドキュメント保護プログラムの構成例を示す図である。

【図 2 0】復号の様子を示す図である。

【図 2 1】ドキュメント印刷プログラムを有したプリンタの構成例を示す図である。

【図 2 2】プリンタが備えるセキュリティ機能の例を示す図である。

【図 2 3】P A C が設定されたドキュメントを印刷する際の処理を示す図である。

【図 2 4】P I N 入力のダイアログを示す図である。

【図 2 5】ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図である。

【図 2 6】ドキュメント保護プログラムをリモートサーバ上に配置した状態を示す図である。

#### 【符号の説明】

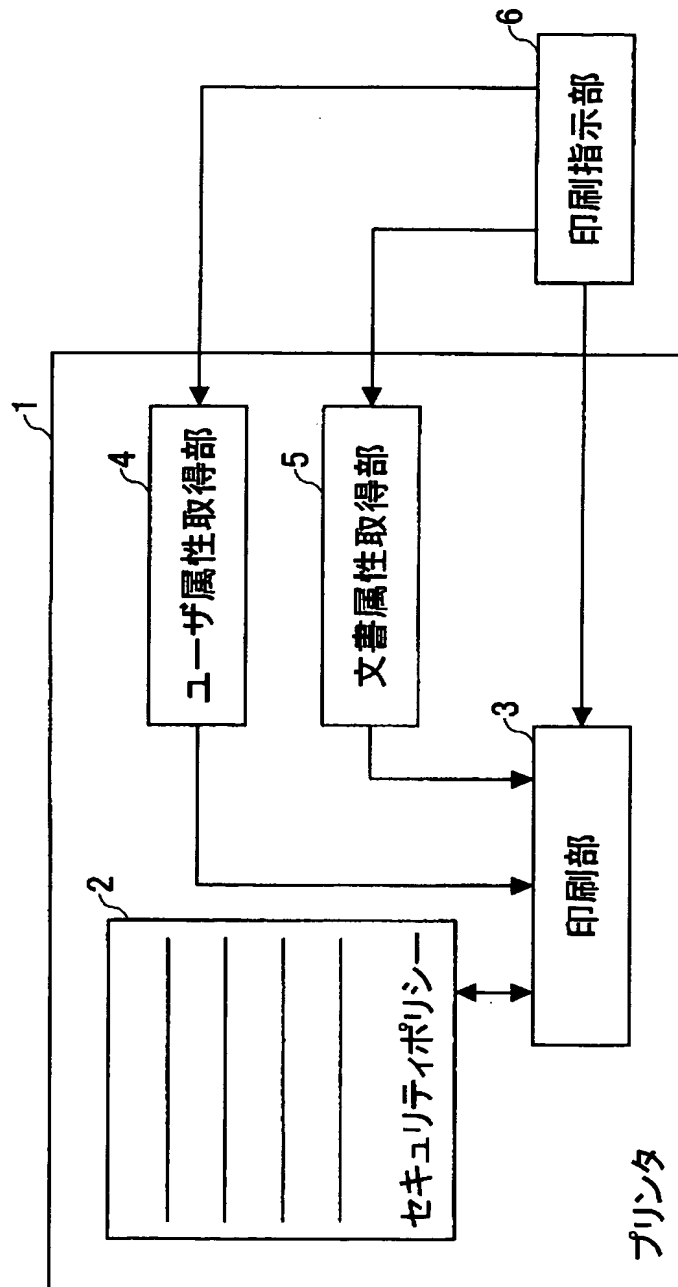
##### 【0 1 5 2】

1	プリンタ
2	セキュリティポリシー
3	印刷部
4	ユーザ属性取得部
5	文書属性取得部
6	印刷指示部
4 0 1	配布者端末
4 0 2	ユーザ端末
4 0 3	プリンタ
4 0 3 a	プリントエンジン
4 0 4	アクセスコントロールサーバ
4 1 1	ドキュメント保護プログラム
4 2 1	ドキュメント印刷プログラム
4 4 1	ユーザデータベース
4 4 3	セキュリティ属性データベース
4 4 4	セキュリティポリシー
4 1 1 a	暗号化部
4 1 1 b	暗号鍵取得部
4 1 1 c	属性付与部
4 1 1 d	属性登録部
4 1 1 e	パラメータ取得部
4 2 1 a	復号部
4 2 1 b	復号鍵取得部
4 2 1 c	印刷要件取得部
4 2 1 d	印刷処理部
4 2 1 e	要件処理部

4 2 1 f ドキュメント加工部  
4 2 1 g プリンタドライバ  
4 2 1 h 警告表示部  
4 2 1 i ログ記録部  
4 2 1 j パラメータ取得部  
4 0 4 a 属性 D B 登録部  
4 0 4 b ユーザ認証部  
4 0 4 c アクセス権限確認部  
4 0 4 d 印刷要件取得送付部

【書類名】 図面  
【図 1】

本発明を好適に実施した第1の実施形態にかかる  
プリンタの内部構成を示す図



【図 2】

セキュリティポリシーの例を示す図

極秘文書について：	
原則複写禁止	複写する際には管理責任者の許可を得なければならない。また、複写したことを記録しておかなければならない。プリントする際には複写禁止であることを示す透かしを入れなければならない。また、プリントしたことを記録しておかなければならない。
閲覧は関係者のみ許可	
丸秘文書について：	
複写は関係者のみ許可	複写する際には丸秘文書であることを示すラベルを同時に印刷しなければならない。
閲覧は関係者のみ許可	
社外秘文書について	
社外へ送付する際には	管理者の許可を得なければならない。
複写・プリント・閲覧は	社内であれば許可不要
人事関連文書について	
全て丸秘文書として扱う	
・	
・	
・	
・	

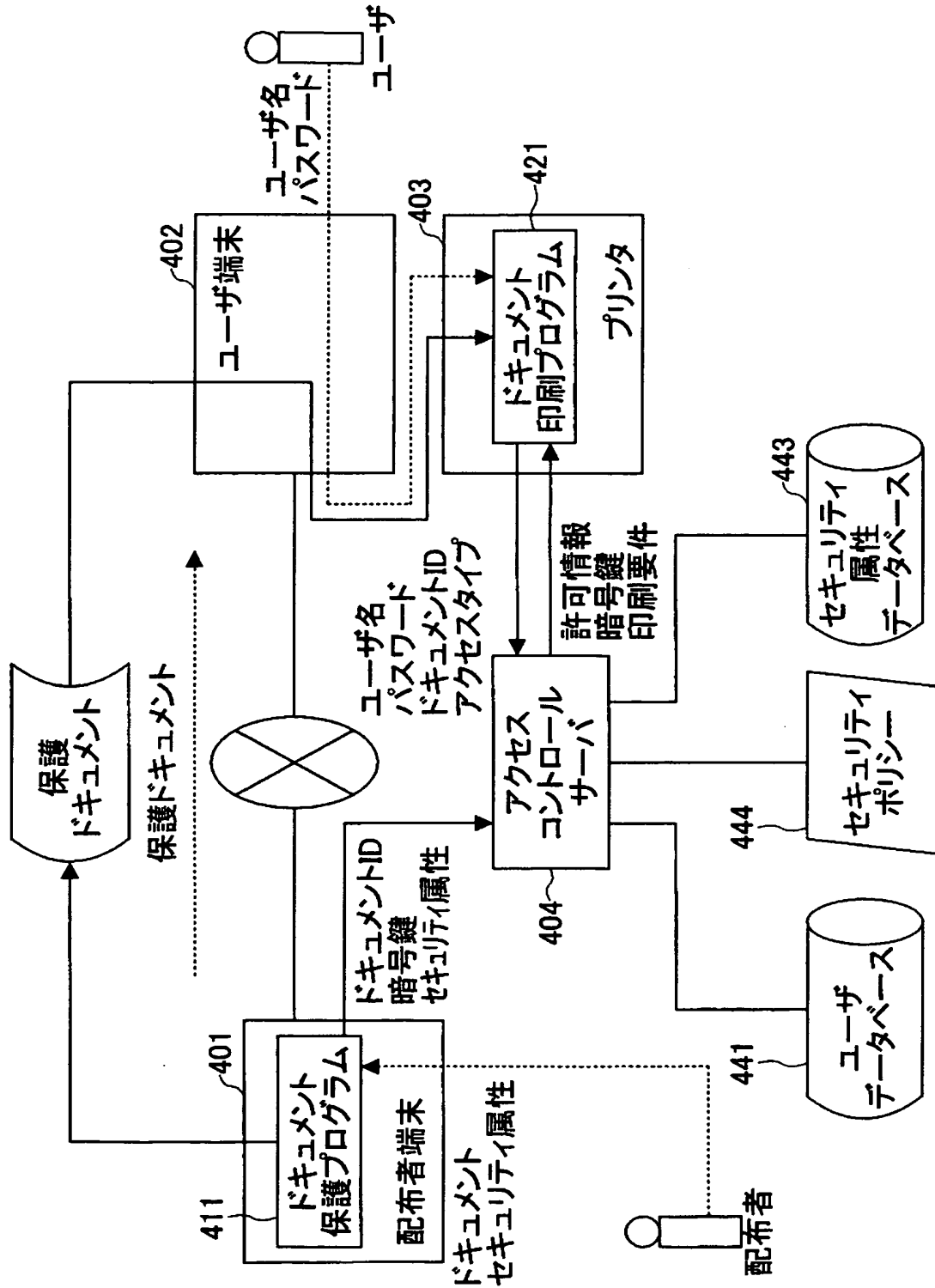
【図 3】

セキュリティポリシーをXML記述により書き表した  
プログラムの例を示す図

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>print</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    <ace>
      <user_category>DOC-CATEGORY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>print</name>
        <requirement>audit</requirement>
        <requirement>embed_trace_info</requirement>
      </operation>
    </ace>
  </acl>
</acc_rule>
</policy>
```

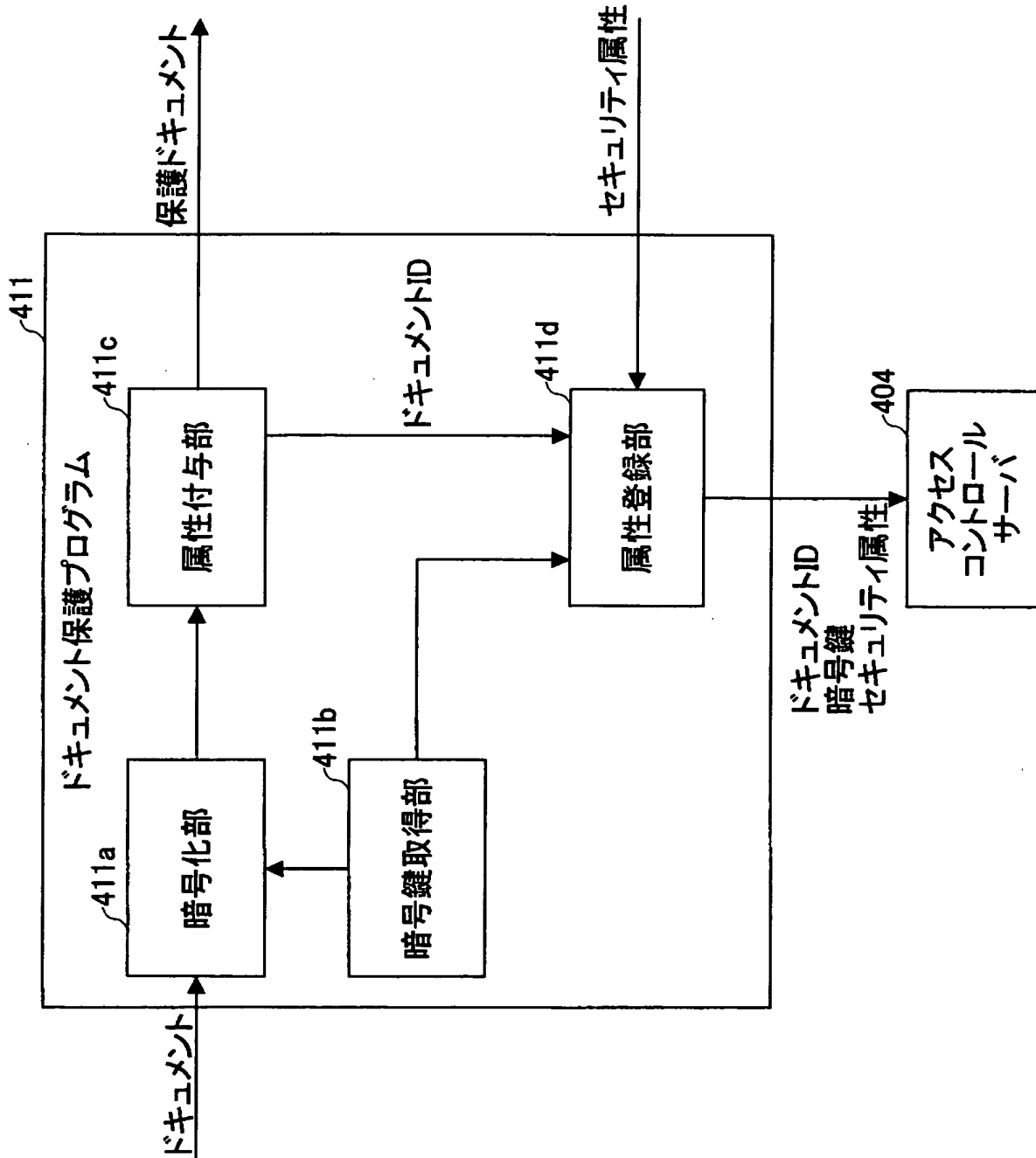
【図 4】

本発明を好適に実施した第2の実施形態にかかる  
ドキュメント保護・印刷システムの構成を示す図



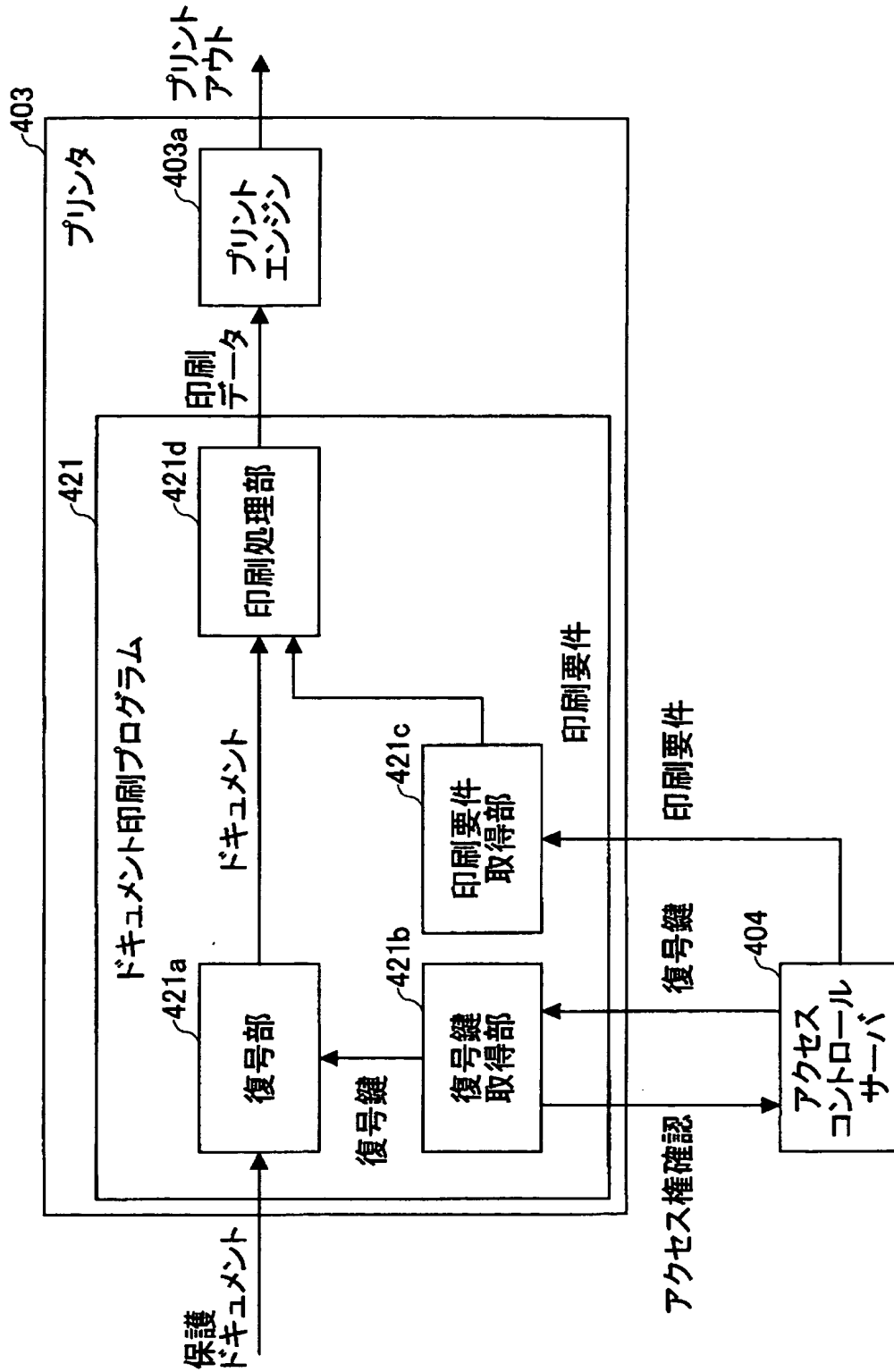
【図 5】

ドキュメント保護プログラムの構成例を示す図



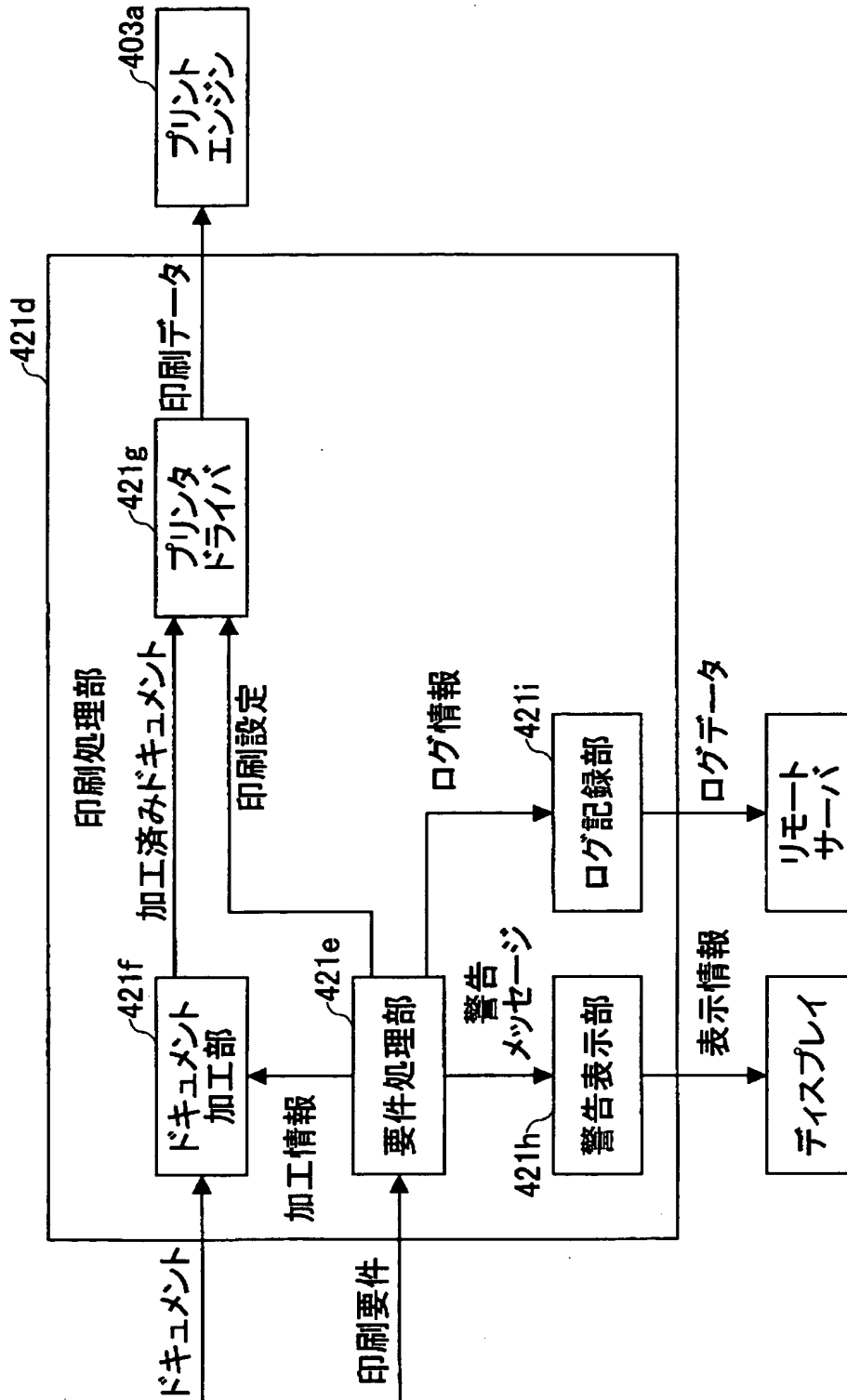
【図 6】

ドキュメント印刷プログラムを有したプリンタの構成例を示す図



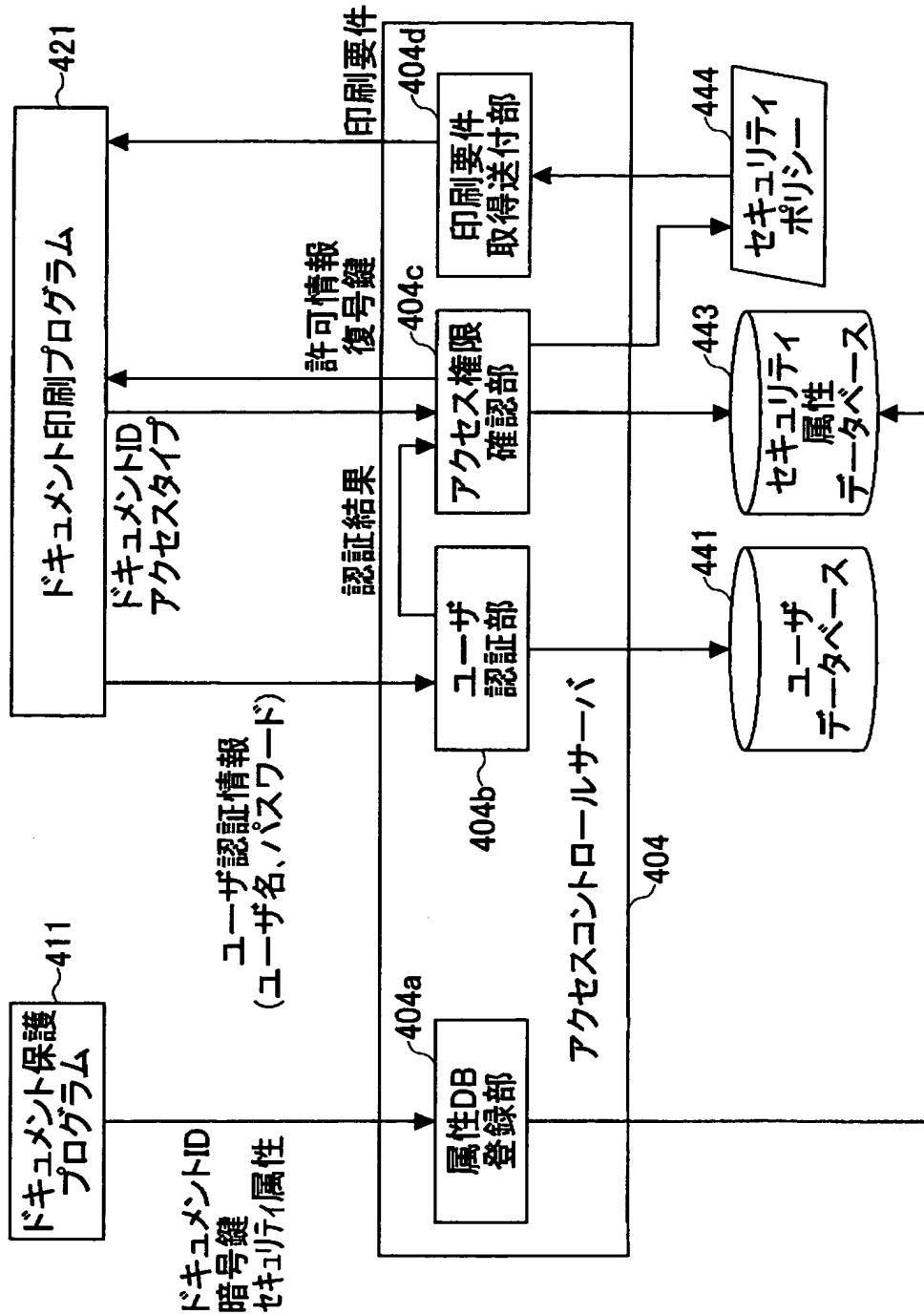
【図 7】

印刷処理部の構成例を示す図



【図 8】

アクセスコントロールサーバの構成例を示す図



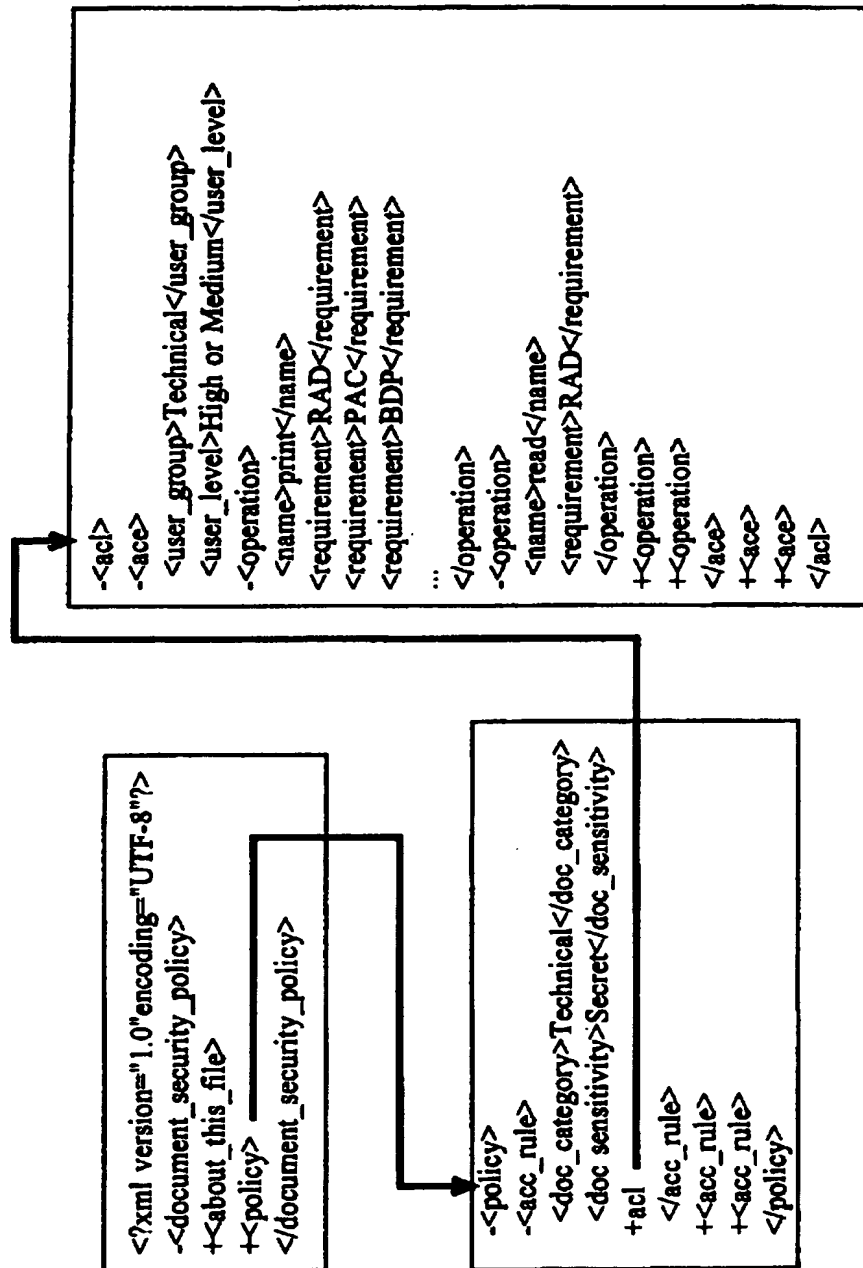
【図 9】

セキュリティポリシーを電子データとした場合のデータ構造を示す図

Document Type		User Type		Access Type	Permission	Requirement
Category	Sensitivity	Category	Level			
Technical	Secret	Technical	Medium High	Read	Allowed	RAD
				Print	Allowed	PAC BDP EBC RAD
				Hardcopy	Denied	
				...		
Technical	Top Secret	Technical	High	...		
Human Resource	Top Secret	Human Resource	High	...		
				Read	Allowed	RAD
				Print	Denied	
				Hardcopy	Denied	

【図 10】

セキュリティポリシーを電子データとして記述した例を示す図



【図 1 1】

ユーザデータベースに記録される情報の構造例を示す図

User name	Password	Category	Level
Ichiro	98q34rah	Technical	Medium
		General	Basic
Taro	Adoijoqer	Human Resource	Top Secret
		General	Basic
⋮			

【図 1 2】

セキュリティ属性の設定を要求する画面の例を示す図

文書のセキュリティ属性

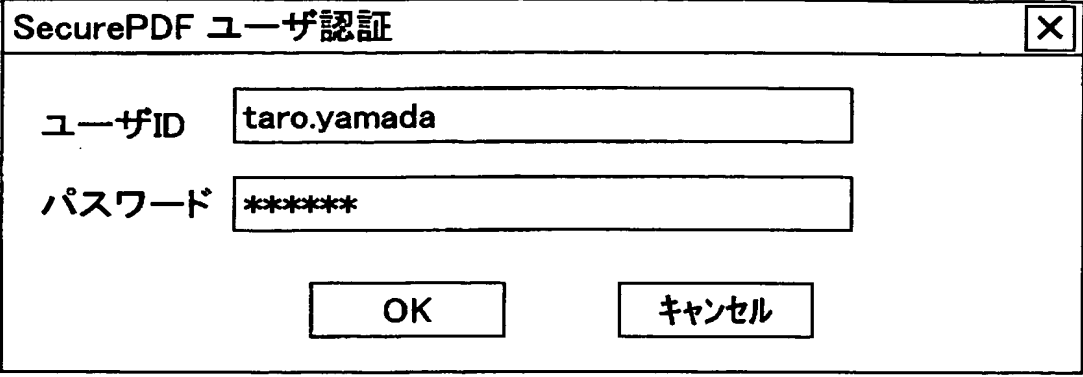
文書カテゴリ

機密レベル

ファイル:

【図 1 3】

ユーザ名(ユーザID)とパスワードを要求する画面の例を示す図

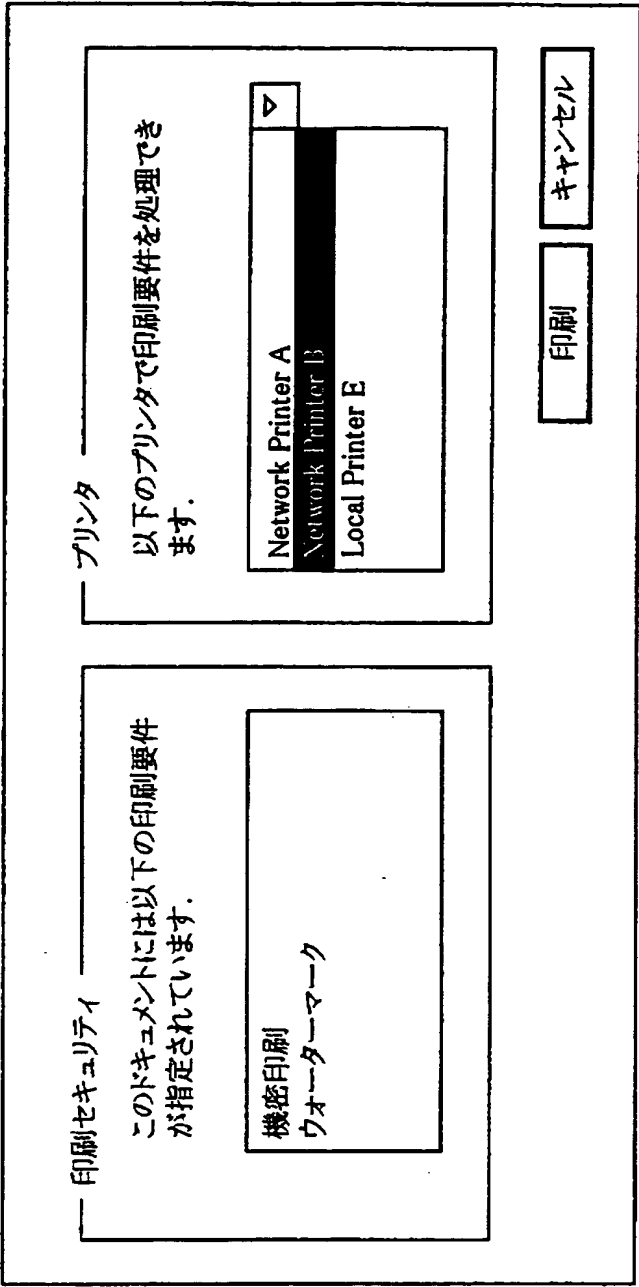


A screenshot of a user authentication dialog box titled "SecurePDF ユーザ認証". The dialog has a standard Windows-style title bar with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first is labeled "ユーザID" and contains the text "taro.yamada". The second is labeled "パスワード" and contains seven asterisks "\*\*\*\*\*". Below the input fields, there are two buttons: "OK" on the left and "キャンセル" (Cancel) on the right.

SecurePDF ユーザ認証	
ユーザID	taro.yamada
パスワード	*****
<div>OK      キャンセル</div>	

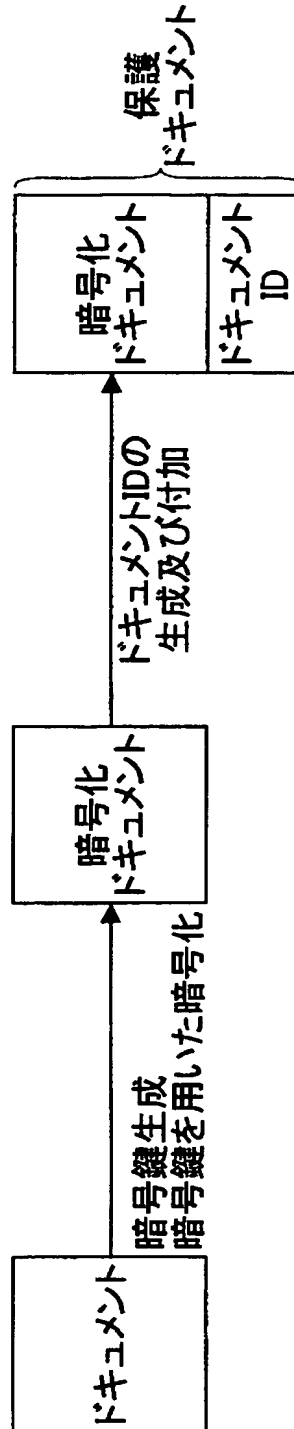
【図 1 4】

ユーザ端末の表示装置上に表示される確認画面の例を示す図

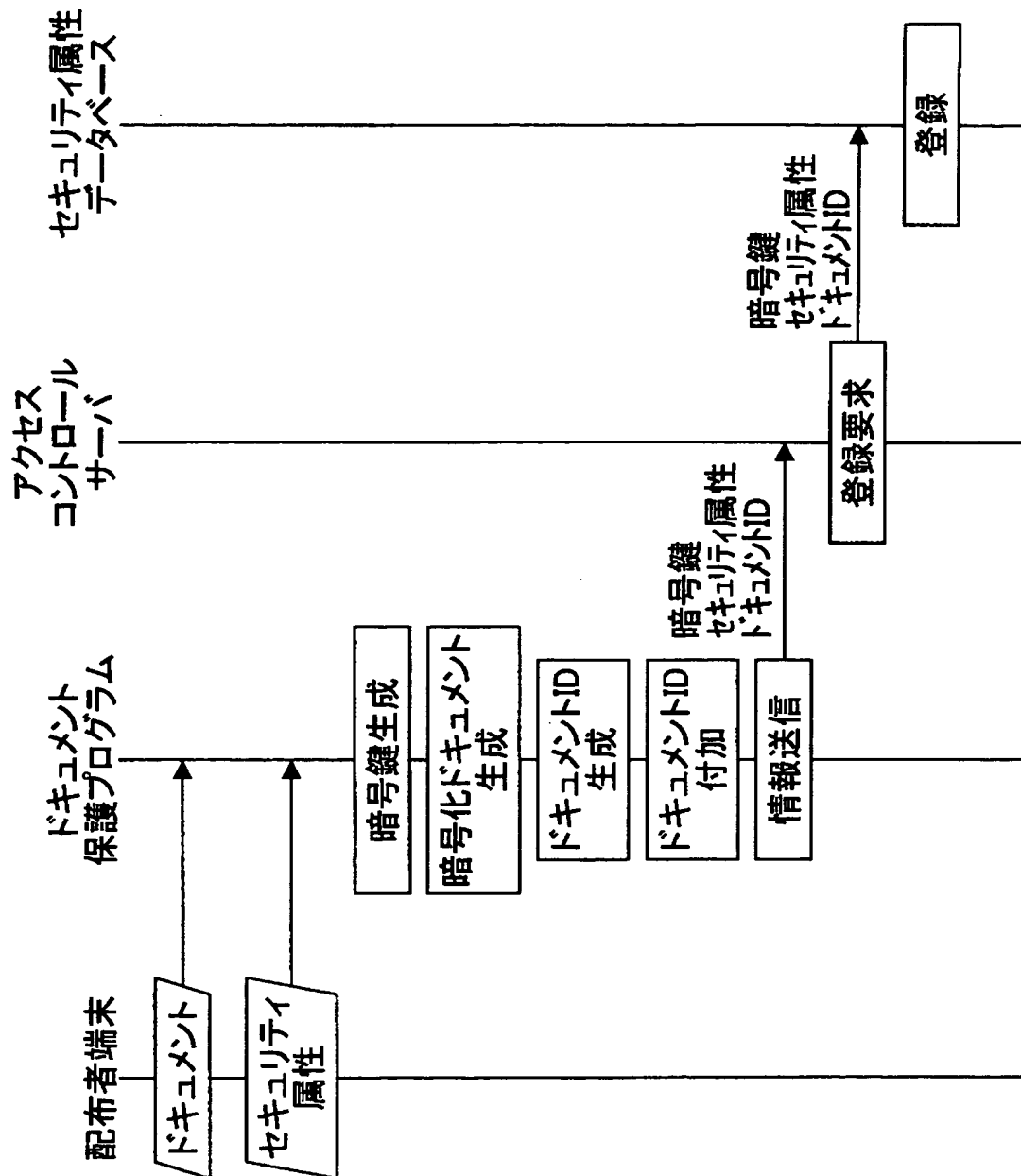


【図 15】

第2の実施形態にかかるドキュメント保護プログラムの処理を示す図

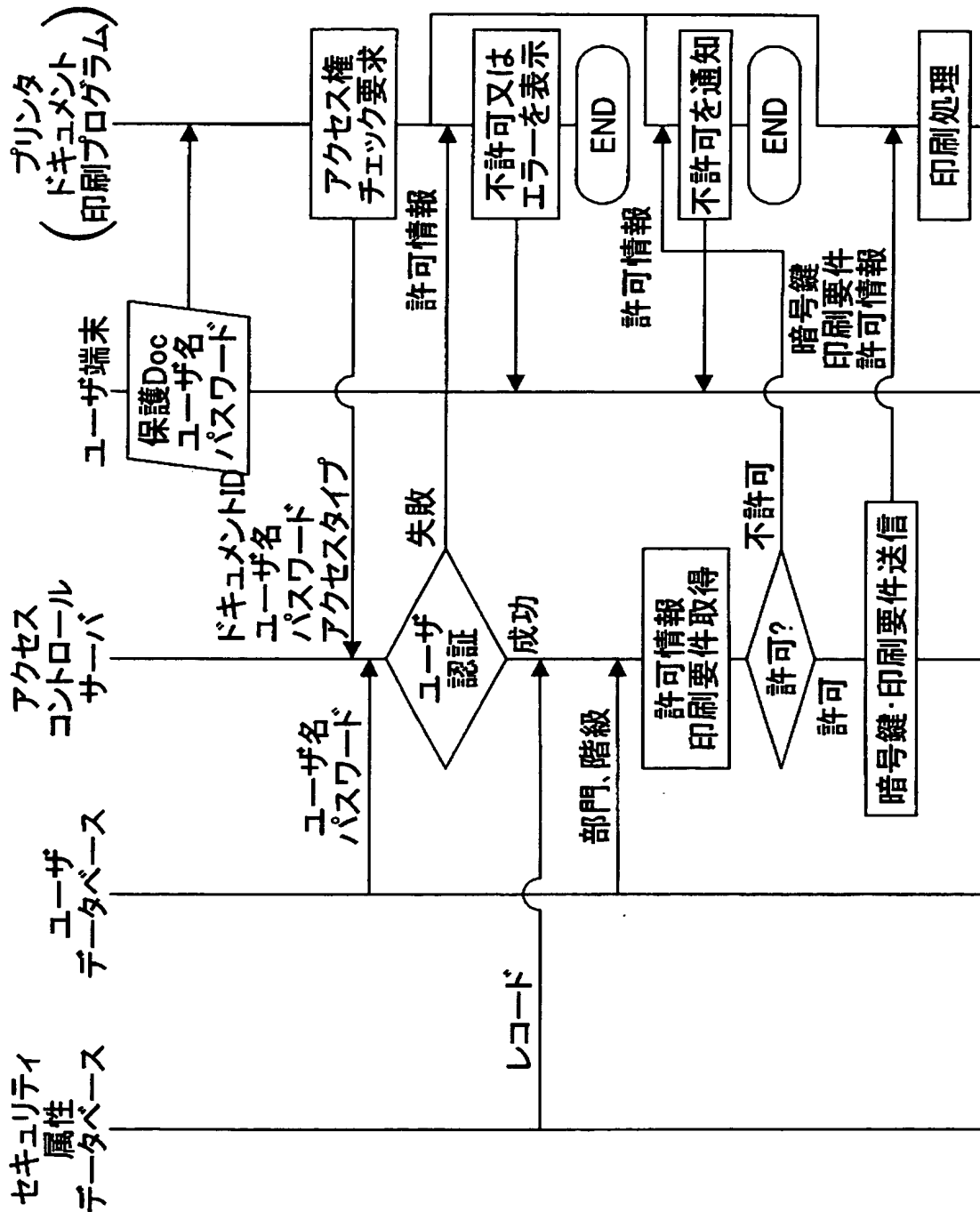


【図 16】

第2の実施形態にかかるドキュメント保護プログラムおよび  
アクセスコントロールサーバの動作の流れを示す図

【図 17】

第2の実施形態にかかるドキュメント印刷プログラムおよび  
アクセスコントロールサーバの動作の流れを示す図



【図 18】

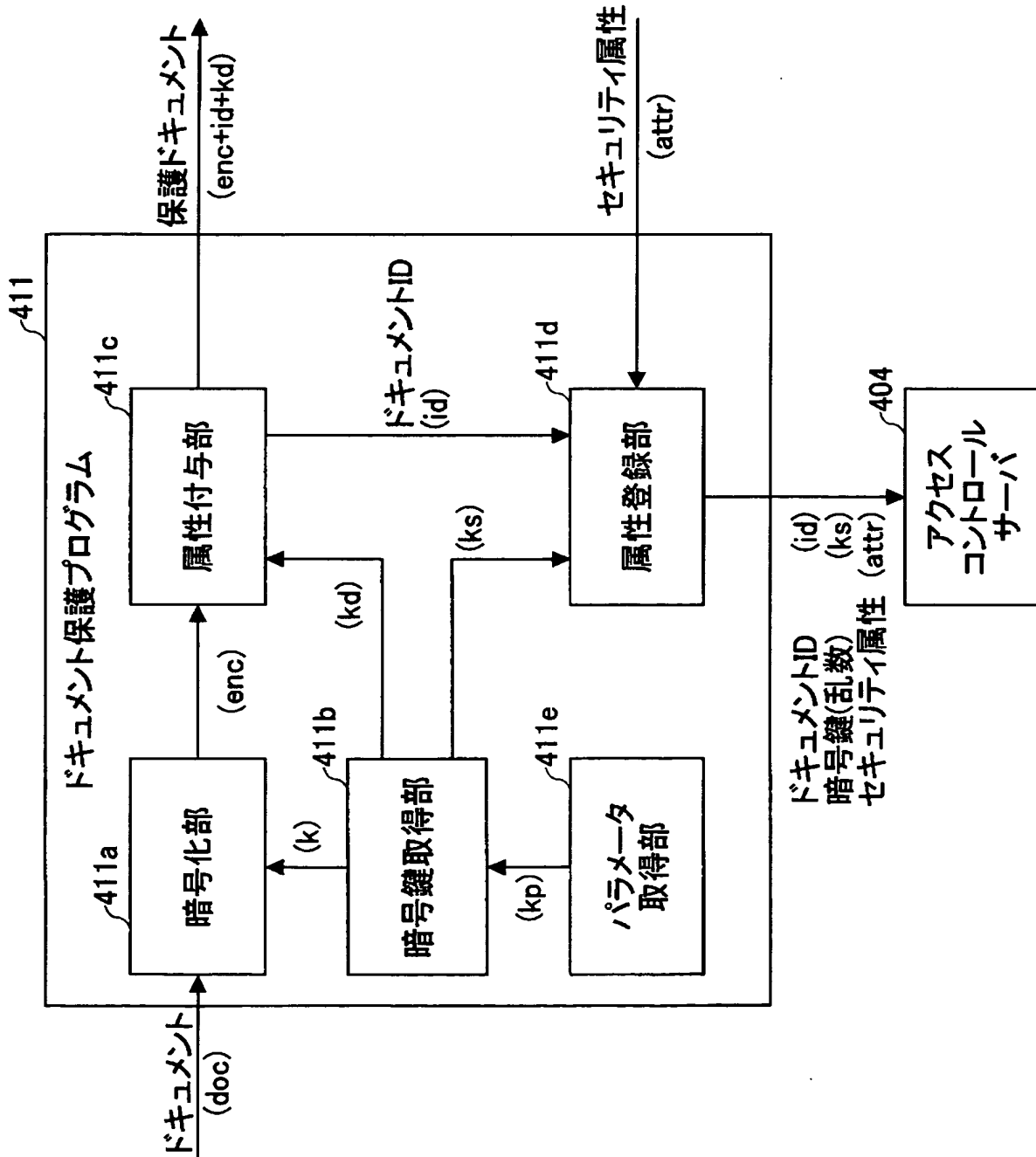
アクセスコントロールサーバへのSOAPによる  
問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowed xmlns:m="http://sample.com/sample">
<sessionId>adfkla;iowoemads</sessionId>
<userId>taro.yamada</userId>
<docId>shm000000000003</docId>
<accessType>print</accessType>
</m:isAllowed>
</s:Body>
</s:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
<isAllowedReturn>
<allowed xsi:type="xsd:boolean">true</allowed>
<requirements>
<item>
<requirement>private_access</requirement>
</item>
<item>
<requirement>watermark</requirement>
<supplement>CONFIDENTIAL</supplement>
</item>
</requirements>
</isAllowedReturn>
</m:isAllowedResponse>
</s:Body>
</s:Envelope>
```

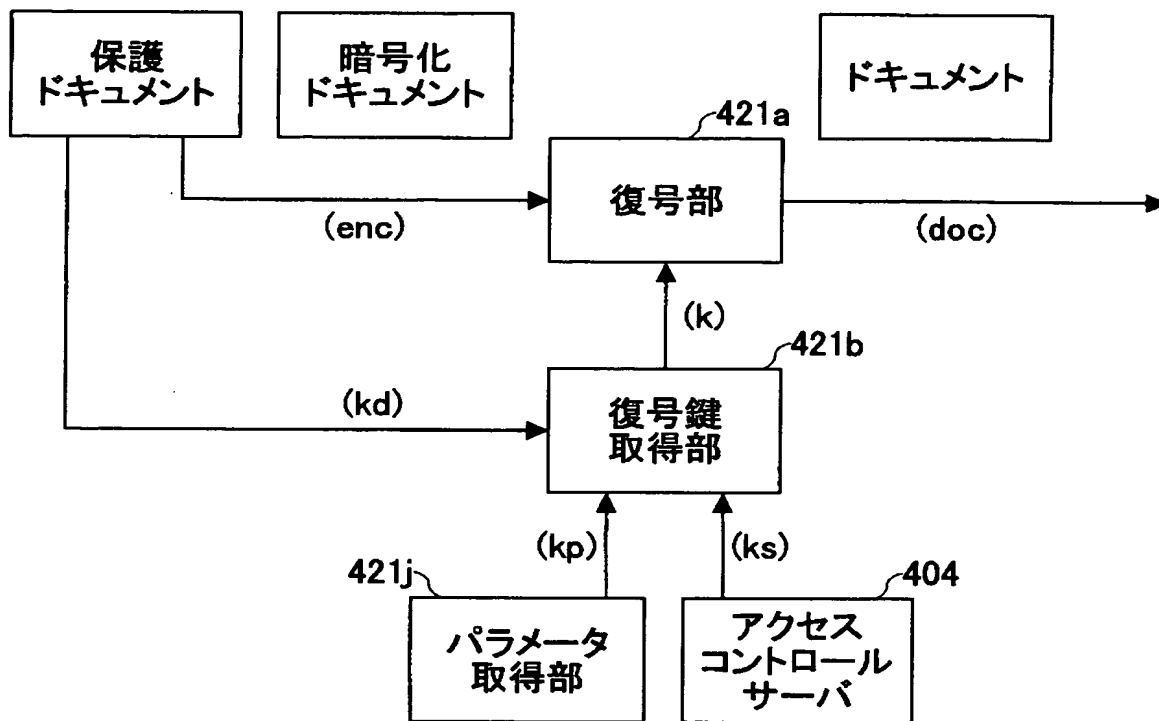
【図 19】

ドキュメント保護プログラムの構成例を示す図



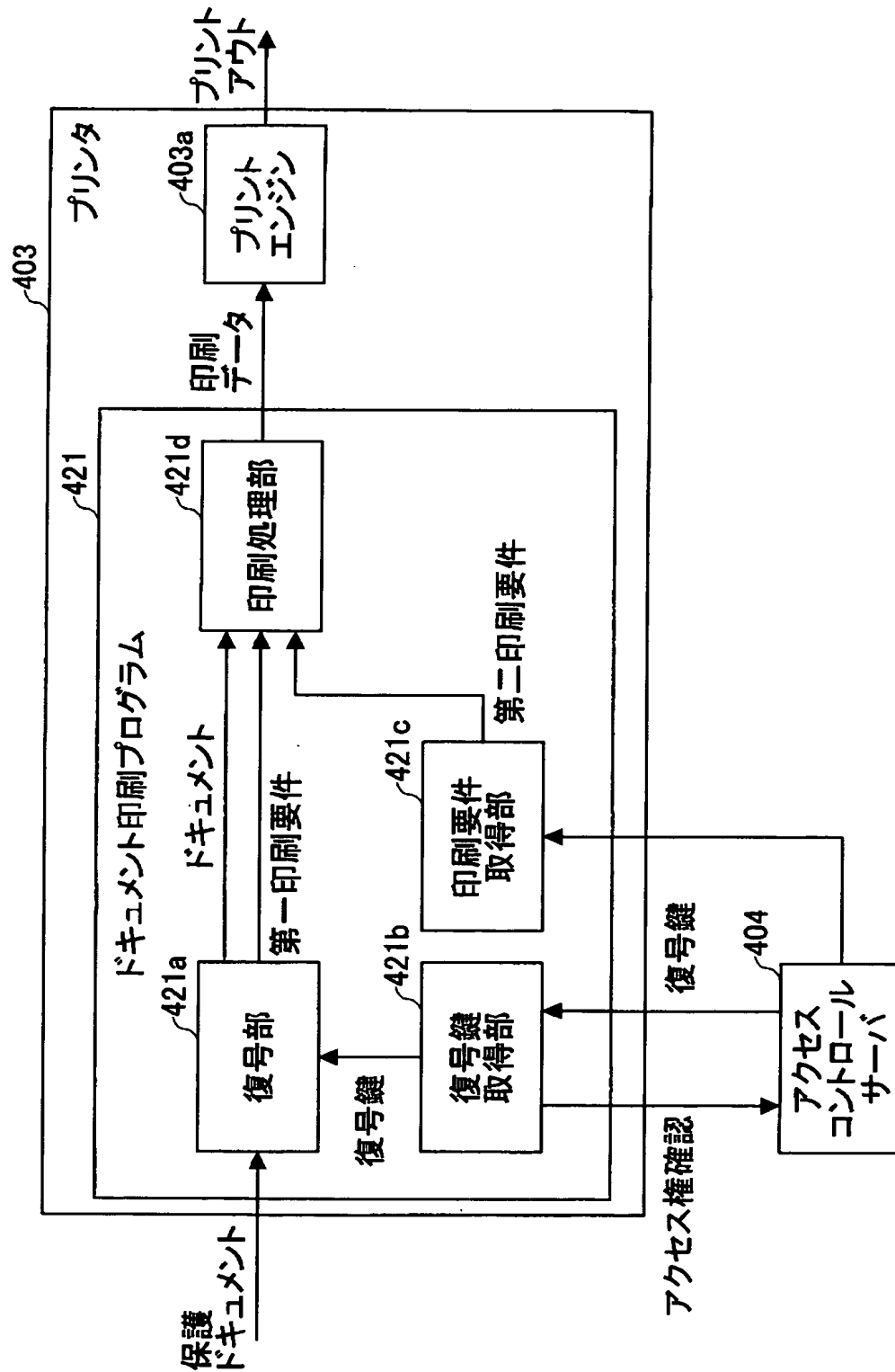
【図 20】

## 復号の様子を示す図



【図 21】

ドキュメント印刷プログラムを有したプリンタの構成例を示す図



【図 22】

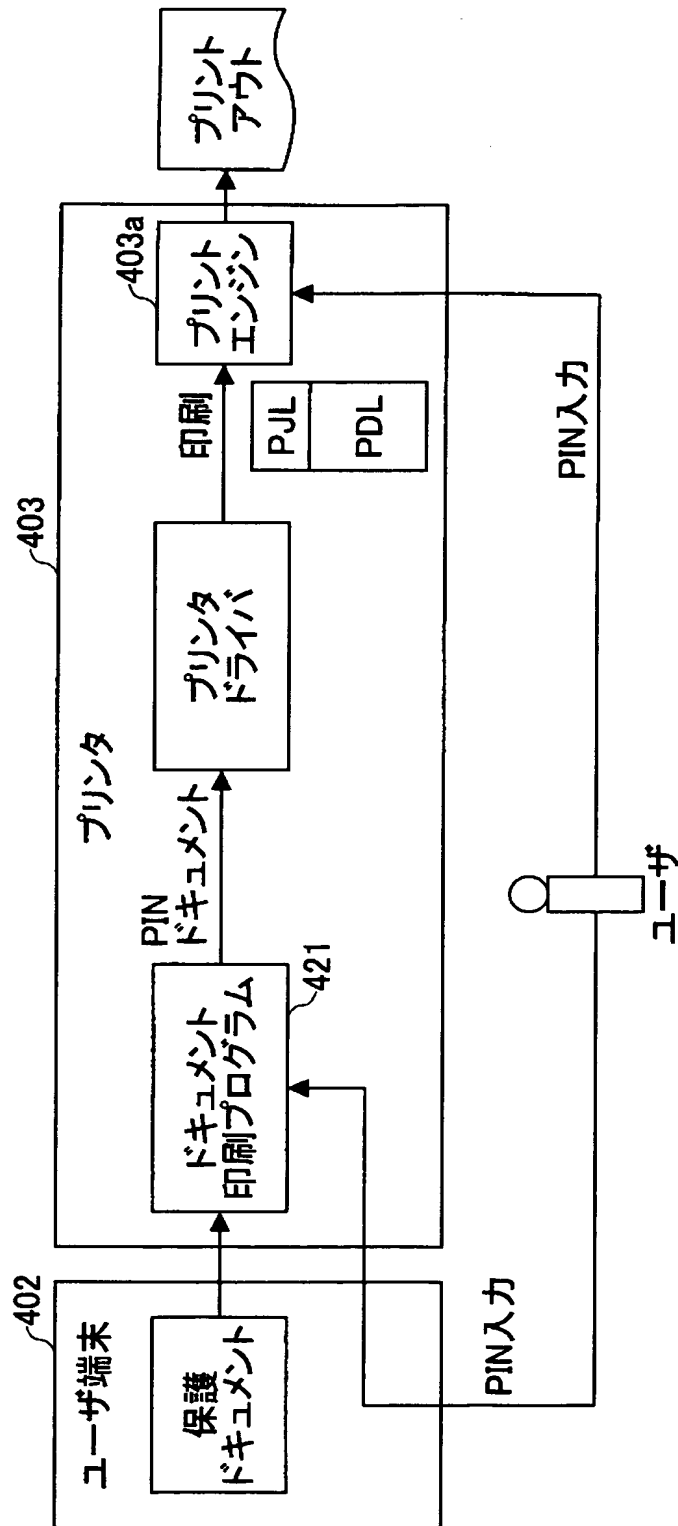
## プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバに P I N (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでその P I N を入力しなければプリントアウトされない機能。

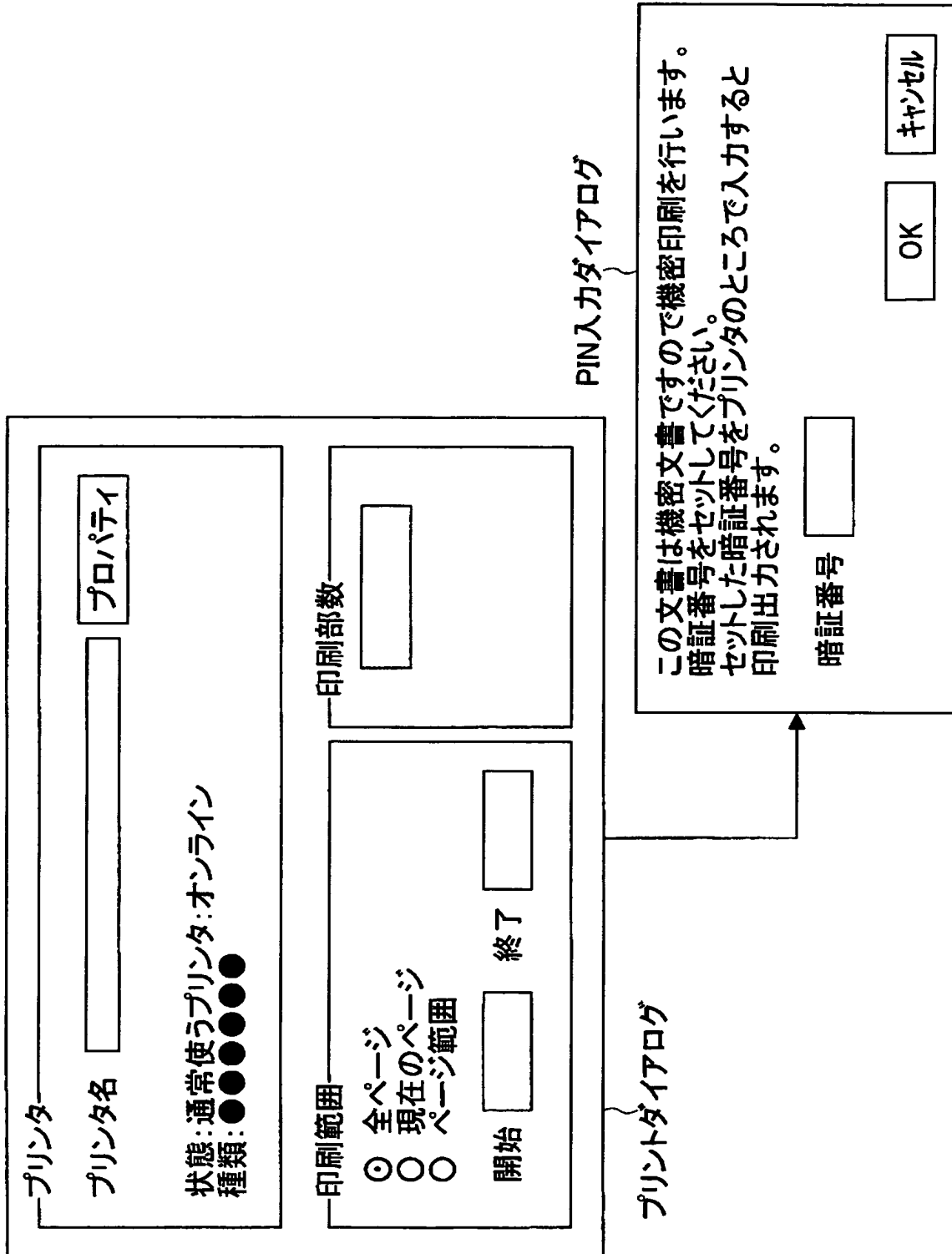
【図 23】

PACが設定されたドキュメントを印刷する際の処理を示す図



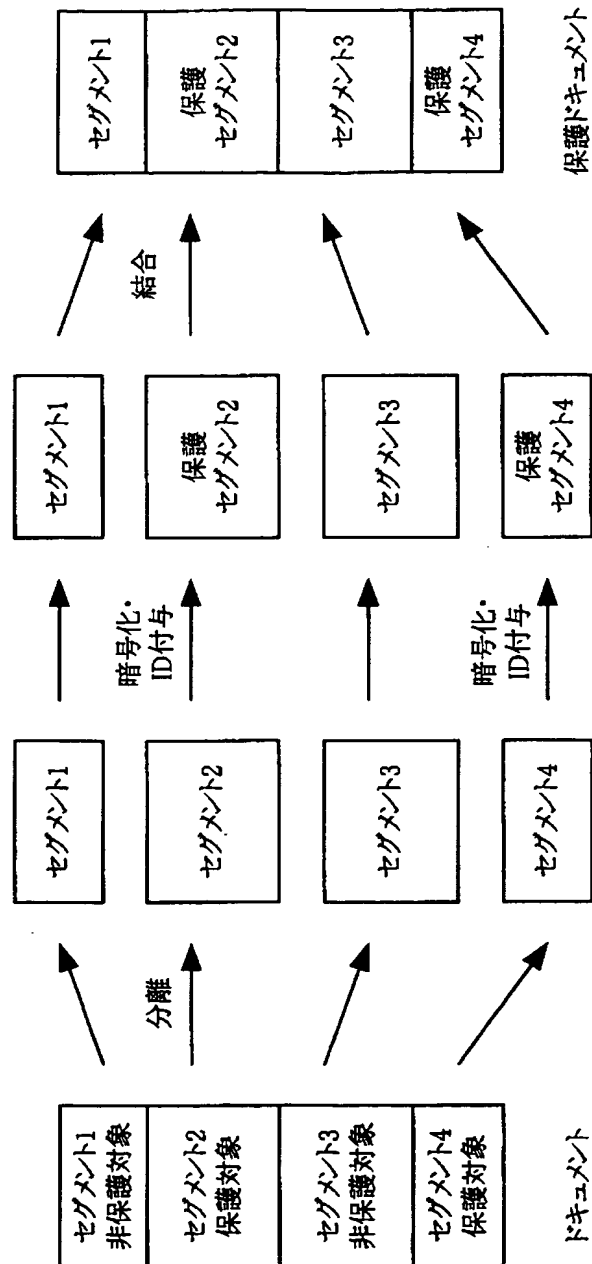
【図 24】

PIN入力のダイアログを示す図



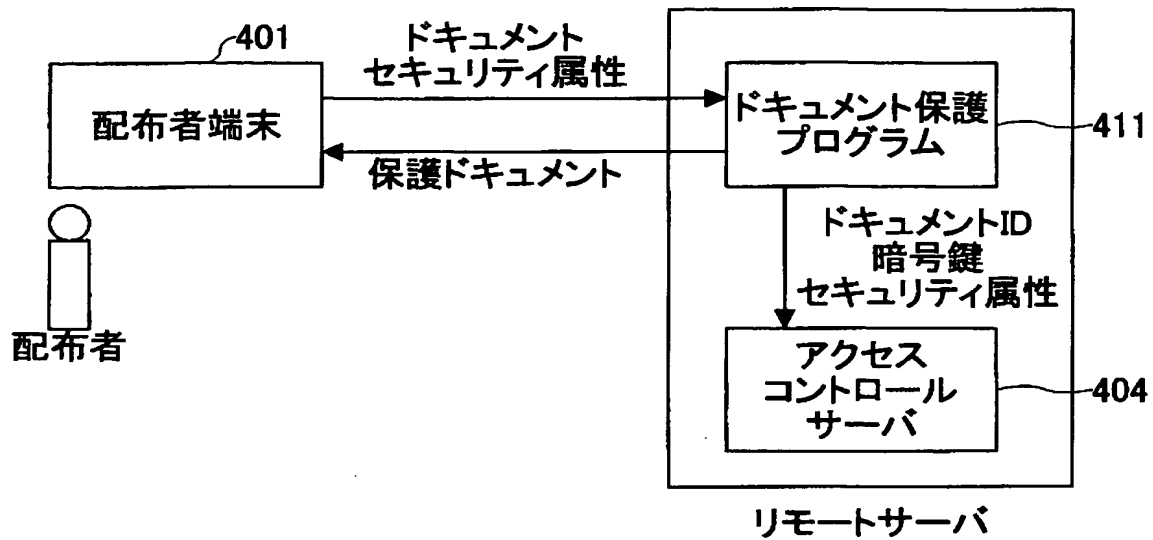
【図 25】

ドキュメントを複数のセグメントに分けて保護する場合の  
処理を示す図



【図 26】

ドキュメント保護プログラムをリモートサーバ上に  
配置した状態を示す図



**【書類名】 要約書****【要約】**

**【課題】** 文書印刷のセキュリティ設定に関して、機器のセキュリティに関する知識が必要である、一つ一つの機器にセキュリティを設定する必要がある、全体のセキュリティ状態が把握できない、実際の文書のセキュリティが守られているかが実感できない、などの問題を解決することを目的とする。

**【解決手段】** ドキュメントファイルの印刷を行うユーザの属性を取得する手段と、上記ドキュメントファイルの属性を取得する手段と、取得した上記ユーザおよび上記ドキュメントファイルの属性に基づき、印刷許否および印刷要件を規定したセキュリティポリシーを検索して印刷要件を取得する手段と、取得した上記印刷要件を印刷時に強制する手段とを備えるドキュメント印刷装置により構成される。

**【選択図】** 図 1

特願 2 0 0 3 - 3 1 4 4 6 8

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 6 7 4 7 ]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー